



744
89/5058/0

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年 2月18日

出願番号
Application Number:

平成11年特許願第039543号

出願人
Applicant(s):

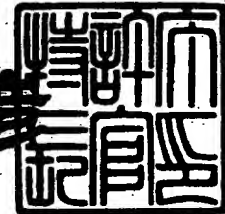
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 2月25日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3010970

特平11-039543

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社

【書類名】 特許願

【整理番号】 2030704064

【提出日】 平成11年 2月18日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 川口 京子

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 高山 久

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 松瀬 哲朗

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 柴田 顕男

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 モバイル・エレクトロニックコマース・システム

【特許請求の範囲】

【請求項 1】

無線通信手段を有する電子財布から、前記無線通信手段を通じて、必要な対価を支払い、供給側から商品やサービスの提供または必要な許可を受けるモバイル・エレクトロニックコマース・システムにおいて、

通信手段を有する指示閲覧手段と、前記電子財布及び前記指示閲覧手段とそれぞれ通信手段を通じて接続するサービス提供手段と、を備え、前記サービス提供手段が、前記指示閲覧手段から受信した購入要求に基づいて、電子バリューを、前記通信手段を通じ無線通信によって前記電子財布にインストールすることを特徴とするモバイル・エレクトロニックコマース・システム。

【請求項 2】

指示閲覧手段から購入要求を受信したサービス提供手段が、電子財布から、購入要求の内容を確認するメッセージを受信した場合に、電子バリューを前記電子財布にインストールすることを特徴とする請求項 1 記載のモバイル・エレクトロニックコマース・システム。

【請求項 3】

サービス提供手段が、電子財布から、購入要求の内容を確認するメッセージを受信した場合に、電子バリューの購入を証明するメッセージを、前記電子財布にインストールすることを特徴とする請求項 1 記載のモバイル・エレクトロニックコマース・システム。

【請求項 4】

購入要求を確認するメッセージが、サービス提供手段から電子財布に送信された購入要求の内容の確認を要求するメッセージに対する応答メッセージであることを特徴とする請求項 2 又は 3 に記載のモバイル・エレクトロニックコマース・システム。

【請求項 5】

サービス提供手段が、指示閲覧手段から受信した購入要求に基づいて発行した

電子バリューを格納する電子バリュー格納手段を有し、前記電子バリュー格納手段に格納された電子バリューを、電子バリューごとに設定された日時に、電子財布にインストールすることを特徴とする請求項 1 から 4 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 6】

サービス提供手段が、
電子財布による電子バリューの購入に伴う対価の支払に対して、電子バリューを生成し、一時的に格納する手段と、
前記電子財布による対価の支払と電子バリューの未領収を証明する引換証を電子財布に発行する発行手段と、
発行された引換証を格納する格納手段を有し、

前記格納手段に格納された引換証に対応する前記電子バリュー格納手段に格納された電子バリューを、電子バリューごとに設定された日時に、前記電子財布にインストールすることを特徴とする請求項 1 から 4 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 7】

サービス提供手段が、指示閲覧手段から受信した購入要求に基づいて発行した電子バリューを格納する電子バリュー格納手段を有し、電子財布から、電子バリューの対価の支払と電子バリューの未領収を証明する引換証を受信した場合に、前記電子バリュー格納手段に格納された前記電子バリューを前記電子財布にインストールすることを特徴とする請求項 1 から 4 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 8】

電子財布が、個人識別情報を送信する個人情報送信手段を有し、サービス提供手段に送信する購入要求に、前記個人情報送信手段から送信された個人識別情報が含まれることを特徴とする請求項 1 から 7 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 9】

供給側が、通信手段を有する電子バリュー決済手段を備え、電子財布から前記

供給側へ対価を支払う手順として、

電子財布が、電子バリューによる対価の支払いを申し出るメッセージを生成し、
前記電子バリュー決済手段へ送信する第一のステップ、

電子バリュー決済手段が、電子財布に、対価の支払いを請求するメッセージを生成し、電子財布へ送信する第二のステップ、

電子財布が、供給側への対価の支払いを証明するメッセージを生成し、電子バリュー決済手段へ送信する第三のステップ、

電子バリュー決済手段が、電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを生成し、電子財布へ送信する第四のステップ、

電子財布が、レシートメッセージを受領したことを証明するメッセージを生成し、電子バリュー決済手段へ送信する第五のステップ、

の5つのステップのうち、1つ以上含むことを特徴とする請求項1から8のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項10】

供給側が、通信手段を有する電子バリュー決済手段を備え、電子財布から前記供給側へ対価を支払う手順として、

電子財布が、電子バリューによる対価の支払いを申し出るメッセージを生成し、指示閲覧手段を介して、前記電子バリュー決済手段へ送信する第一のステップ、
電子バリュー決済手段が、対価の支払いを請求するメッセージを生成し、指示閲覧手段を介して、電子財布へ送信する第二のステップ、

電子財布が、供給側への対価の支払いを証明するメッセージを生成し、指示閲覧手段を介して、電子バリュー決済手段へ送信する第三のステップ、

電子バリュー決済手段が、電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを生成し、指示閲覧手段を介して、前記電子財布へ送信する第四のステップ、

の4つのステップのうち、1つ以上含むことを特徴とする請求項1から8のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項11】

指示閲覧手段からサービスの提供を要求された供給側が、電子財布から電子バリューによる対価の支払いが行われた場合に、前記指示閲覧手段に対して前記サービスを提供することを特徴とする請求項 1 から 1 0 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 1 2】

指示閲覧手段が、供給側から提供されたサービスの履歴を格納する履歴情報格納手段を有し、電子財布が、前記履歴情報格納手段に格納された履歴情報に基づいて、前記供給側に電子バリューによる対価の支払いを行うことを特徴とする請求項 1 から 1 1 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 1 3】

指示閲覧手段が、履歴情報格納手段に格納された履歴情報を送信する手段を有し、電子財布が、電子バリューにより、供給側へ対価を支払う際に送信するメッセージの中に、前記指示閲覧手段から前記電子財布に送信された履歴情報が含まれることを特徴とする請求項 1 2 記載のモバイル・エレクトロニックコマース・システム。

【請求項 1 4】

指示閲覧手段が、放送受信手段を有し、電子財布から供給側への電子バリューによる対価の支払に対して、前記供給側が、前記放送受信手段による放送の視聴を可能にする情報を前記指示閲覧手段に送信することを特徴とする請求項 1 から 1 3 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 1 5】

放送受信手段による放送の視聴を可能にする情報の中に、放送の復号化処理に用いる鍵情報が含まれていることを特徴とする請求項 1 4 に記載のモバイル・エレクトロニックコマース・システム。

【請求項 1 6】

放送の復号化処理に用いる鍵情報が、放送のスクランブルを解除するスクランブル鍵にかけられた暗号を復号化する暗号鍵であることを特徴とする請求項 1 5 に記載のモバイル・エレクトロニックコマース・システム。

【請求項 17】

供給側から供給されるサービスが、インターネットやパソコン通信などの通信回線を用いたネットワーク情報サービスであることを特徴とする請求項 1 から 16 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 18】

供給側から供給されるサービスが、放送サービスであることを特徴とする請求項 14 から 16 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 19】

供給側から供給されるサービスが、ネットワーク情報サービスと放送サービスの組み合わせであることを特徴とする請求項 14 から 16 のいずれかに記載のモバイル・エレクトロニックコマース・システム。

【請求項 20】

無線通信手段を有する電子財布から、前記無線通信手段を介した供給側への支払に対して、指示閲覧手段から供給側に要求した、

- (1) 電子財布への電子バリューのインストールするサービス
- (2) 指示閲覧手段へのネットワーク情報サービス
- (3) 指示閲覧手段への放送サービス
- (4) 物品の販売をするサービス
- (5) 前記(1)から(4)の任意の組合せ

といったサービスが提供されることを特徴とするモバイル・エレクトロニックコマース・システム。

【請求項 21】

無線通信手段と、支払と電子バリューの未領収を証明する引換証を格納する格納手段とを有し、

前記格納手段に格納された引換証に対応する電子バリューのインストールを、前記無線通信手段を介して、所定の機関に要求する手段を有することを特徴とする電子財布。

【請求項 22】

通信手段を有し、前記通信手段を介し、供給側へ対価を支払う手順として、
 対価の支払いを申し出るメッセージを供給側へ送信する第一のステップ、
 供給側から、対価の支払いを請求するメッセージを受信する第二のステップ、
 供給側への対価の支払いを証明するメッセージを供給側へ送信する第三のステップ、
 供給側から、電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを受信する第四のステップ、
 レシートメッセージを受領したことを証明するメッセージを供給側へ送信する第五のステップ、
 の5つのステップのうち、1つ以上含むことを特徴とする電子財布。

【請求項 23】

通信手段を有し、前記通信手段を用いて、指示閲覧手段を介して供給側へ対価を支払う手順として、
 対価の支払いを申し出るメッセージを指示閲覧手段へ送信する第一のステップ、
 対価の支払いを請求するメッセージを、指示閲覧手段から受信する第二のステップ、
 供給側への対価の支払いを証明するメッセージを指示閲覧手段へ送信する第三のステップ、
 電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを、指示閲覧手段から受信する第四のステップ、
 の4つのステップのうち1つ以上含むことを特徴とする電子財布。

【請求項 24】

通信手段が、無線通信手段であることを特徴とする請求項 22 または 23 に記載の電子財布。

【請求項 25】

無線通信手段を有し、指示閲覧手段に提供されるサービスの対価を、前記無線通信手段を介して提供側に支払う手段を有する電子財布。

【請求項 26】

提供側に、指示閲覧手段に提供されるサービスの対価を支払うことを特徴とする

る、請求項 2 2 から 2 4 のいずれかに記載の電子財布。

【請求項 2 7】

取引の識別情報を入力する入力手段を有し、前記入力手段で入力された識別情報を供給側に送信する手段を有することを特徴とする請求項 2 5 または 2 6 に記載の電子財布。

【請求項 2 8】

取引の識別情報を入力する入力手段を有し、前記入力手段で入力された識別情報が、供給側に対価を支払う際に送信するメッセージに含まれることを特徴とする請求項 2 2 から 2 7 のいずれかに記載の電子財布。

【請求項 2 9】

入力手段が、無線通信によって指示閲覧手段から取引の識別情報を取得する手段であることを特徴とする請求項 2 8 に記載の電子財布。

【請求項 3 0】

取引の識別情報が、指示閲覧手段と指示閲覧手段に提供されるサービスを識別する情報であることを特徴とする請求項 2 7 から 2 9 のいずれかに記載の電子財布。

【請求項 3 1】

電子バリューを格納する格納手段を有し、指示閲覧手段に提供されるサービスの対価を、前記格納手段に格納された電子バリューにより供給側に支払うことを特徴とする請求項 2 0 から 3 0 のいずれかに記載の電子財布。

【請求項 3 2】

電子バリューを格納する格納手段を有し、指示閲覧手段に提供されたサービスの対価を、前記指示閲覧手段に格納された履歴情報に基づいて、前記格納手段に格納された電子バリューにより供給側に支払うことを特徴とする請求項 2 0 から 3 1 のいずれかに記載の電子財布。

【請求項 3 3】

指示閲覧手段から、前記指示閲覧手段に格納された履歴情報を受信する受信手段を有し、前記受信手段で受信した履歴情報を、供給側に送信する手段を有することを特徴とする請求項 2 0 から 3 3 のいずれかに記載の電子財布。

【請求項 3 4】

指示閲覧手段から、前記指示閲覧手段に格納された履歴情報を受信する受信手段を有し、供給側に対価を支払う際に送信するメッセージの中に、前記受信手段で受信した履歴情報が含まれることを特徴とする請求項 2 0 から 3 2 のいずれかに記載の電子財布。

【請求項 3 5】

指示閲覧手段に、提供側から受信した支払処理の結果を送信する送信手段を有することを特徴とする請求項 3 3 または 3 4 に記載の電子財布。

【請求項 3 6】 無線通信手段と、

提供されたサービスの対価の支払を、前記無線通信手段を介して電子財布に要求する支払要求手段と、を有する指示閲覧手段。

【請求項 3 7】 通信手段と、

前記通信手段を介して、供給側にサービスを要求する手段と、供給側に対するサービスの対価の支払を、無線通信手段を介して電子財布に要求する手段と、を有する請求項 3 6 に記載の指示閲覧手段。

【請求項 3 8】

供給側に要求するサービスが、通信手段を介して提供されるネットワーク情報サービスであることを特徴とする請求項 3 7 に記載の指示閲覧手段。

【請求項 3 9】

放送受信手段を有し、供給側に要求するサービスが、前記通信手段を介して提供される放送を視聴可能にする情報の提供であることを特徴とする請求項 3 7 に記載の指示閲覧手段。

【請求項 4 0】

通信手段と、前記通信手段を介して供給側からチャンネル鍵を取得するチャンネル鍵取得手段と、取得したチャンネル鍵を格納するチャンネル鍵格納手段と、前記チャンネル鍵格納手段に格納されたチャンネル鍵を用いてスクランブル鍵にかけられた暗号を解除するスクランブル鍵復号手段と、復号化されたスクランブル鍵を用いて放送のスクランブルを解除する放送受信手段とを有する請求項 3 6 から 3 9 のいずれかに記載の指示閲覧手段。

【請求項 4 1】

ＩＣカード読み書き手段を有し、チャンネル鍵格納手段と、スクランブル鍵復号手段とを、前記ＩＣカード読み書き手段に装着されたＩＣカード上に備えることを特徴とする請求項 4 0 に記載の指示閲覧手段。

【請求項 4 2】

スクランブル鍵格納手段に格納されたスクランブル鍵の復号化を、ＩＣカード上で行うことを特徴とする請求項 4 1 に記載の指示閲覧手段。

【請求項 4 3】

提供されたサービスの履歴を格納する履歴格納手段と、前記履歴格納手段に格納された履歴情報に基づいて、電子財布に、対価の支払を要求する支払要求手段と、を有する指示閲覧手段。

【請求項 4 4】

支払要求手段で行った要求に対する処理結果を受信する受信手段と、前記受信手段で受信した処理結果に基づいて、前記履歴格納手段に格納された履歴情報を変更する手段と、を有する請求項 4 3 に記載の指示閲覧手段。

【請求項 4 5】

履歴情報格納手段に格納される履歴情報が、放送を視聴した場合に格納されることを特徴とする請求項 4 3 又は 4 4 に記載の指示閲覧手段。

【請求項 4 6】

請求項 1 から 3 5 のいずれかに記載の電子財布の中央処理装置の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 4 7】

請求項 1 から 1 9 のいずれかに記載の電子バリュー決済手段の中央処理装置の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 4 8】

請求項 1 から 1 9 のいずれか、および請求項 3 6 から 4 5 のいずれかに記載の指示閲覧手段の中央処理装置の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 49】

請求項 1 から 19 のいずれかに記載のサービス提供手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プリペイドカードやクレジットカード（バンクカード）に代表される小売販売取引における決済機能、及び、移動体電話用のテレホンカードによる通話料金の決済機能、各種イベント、公演、映画等のチケットの改札機能、さらには、それら、プリペイドカードやテレホンカード、チケットの流通・販売機能を提供するエレクトロニックコマースシステムに関し、特に、利便性と、決済の安全性を担保し、効率的で、円滑な商取引を可能にするものである。

【0002】

【従来の技術】

近年、テレホンカードや、パチンコカード等のプリペイドカードの普及により、磁気カードを用いた、前払い方式による決済は、一つの決済方式として、一般的なものになっている。しかし、一方で、変造カードや、販売店による不正請求などのトラブルも増えており、決済システムとしての安全性の向上が求められている。最近では、不正防止対策の一つとして、ICカードタイプのプリペイドカードも登場している。

以下では、ICカードタイプのプリペイドカードも含めた、従来のプリペイドカードによる決済システムについて説明する。

【0003】

図 28（a）は、従来の一般的なプリペイドカードを用いた、前払い方式による決済システムの構成を示すものである。

図 28（a）において、プリペイドカード端末 2601 は、小売販売店 2606 に設置され、販売店でのプリペイドカードによる決済を行なう端末である。プリペイドカ

ード端末2601は、通信回線2604を介して、プリペイドカード発行者2607のセンターシステム2602に接続されている。販売店によっては、プリペイドカード端末2601は、販売店のPOSシステム、及び、通信回線2604を介して、プリペイドカード発行者2607のセンターシステム2602に接続される。

【 0 0 0 4 】

プリペイドカードを用いて、小売販売店2606で商品を購入する場合、まず、消費者2605は、プリペイドカードを販売するプリペイドカード販売店2603で、現金を支払い（2608）、プリペイドカード2600を購入する（2609）。この時のプリペイドカードの売上は、プリペイドカード販売店2603から、プリペイドカード発行者2607に送られる（2610）。

【 0 0 0 5 】

次に、消費者2605は、小売販売店2606において、店員にプリペイドカード2600を渡し（2611）、プリペイドカードによる決済を依頼する。

店員は、プリペイドカード2600をプリペイドカード端末2601のカードリーダーに挿入し、プリペイドカード決済の操作を行なう。すると、プリペイドカード端末2601は、プリペイドカード2600から、残高情報を読み出し、それから商品代金を差し引いた、新しい残高情報を、プリペイドカードに書き込む。そして、プリペイドカード端末2601は、代金計算の明細と、プリペイドカードの新しい残高とを示す計算書をプリンタから印字する。

店員は、購入された商品と、プリペイドカードと計算書を、消費者2605に引き渡し（2613、2612）、プリペイドカードによる決済を終了する。

【 0 0 0 6 】

この後、プリペイドカード端末2601は、通信回線2604を介して、プリペイドカード2600から差引いた金額をもとに、プリペイドカード発行者2607のセンターシステム2602に支払を請求し（2614）、それに対して、プリペイドカード発行者2607から、小売販売店2606に支払が行われる（2615）。

【 0 0 0 7 】

プリペイドカードは、プリペイドカードを販売する自動販売機から購入する場合もあり、また、プリペイドカード端末2601が、プリペイドカードによる決済機

能を有する自動販売機や公衆電話の場合であっても、基本的な仕組みは同じである。

【 0 0 0 8 】

また、安全対策の一つとして、特公平 6 - 1 0 3 4 2 6 号公報に開示されているように、プリペイドカードとカードリーダーライタとの間で、デジタル署名を用いた相互認証を行なうシステムも提案されている。

また、プリペイドカードと同じように、前払い決済を行なう各種のイベントや、公演、映画等のチケットの販売と、その使用について考えてみると、チケットの発券は、オンラインによって行われているが、チケットの改札は、係員の目視によって行われている。

【 0 0 0 9 】

図 2 8 (b) は、従来の一般的なチケットの販売システムの構成を示すものである。

図 2 8 (b) において、チケット発券端末 2617 は、チケット販売店 2620 に設置され、チケットの発券処理を行なう端末である。チケット発券端末 2617 は、通信回線 2619 を介して、チケット発行者 2621 のセンターシステム 2618 に接続されている。

各種イベントや、公演、映画等のチケットを購入する場合、消費者 2605 は、まず、チケット発行者 2621 のセンターシステム 2618 に電話をかけ、希望のチケットの予約を行なう (2624) 。センターシステム 2618 は、申込まれたチケットの予約処理を行ない、消費者 2605 に予約番号を発行する (2625) 。

予約番号の発行を受けた消費者 2605 は、次に、チケット販売店 2620 へ行き、店員に、予約番号を伝え、チケットの発券を依頼する。

【 0 0 1 0 】

店員は、チケット発券端末 2617 に、予約番号を入力して、チケットの発券操作を行なう。すると、チケット発券端末 2617 は、通信回線 2619 を介して、予約番号をチケット発行者 2621 のセンターシステム 2618 へ送信し (2627) 、それに対して、センターシステム 2618 から、予約されていたチケットのチケット情報が、チケット発券端末 2617 へ送信される (2628) 。

チケット発券端末2617は、受信したチケット情報を、チケット発行者2621が定める特定の台紙に印字し、チケット2616として出力する。店員は、現金と引き換えに（2629）、発券したチケット2616を、消費者2605に渡し（2630）、チケットの販売を終了する。

この時のチケットの売上げは、チケット販売店2620の手数料を差引いて、チケット発行者2621へ送られ、さらに、チケット発行者2621の手数料を差引いて、販売したチケットのイベント興行主に支払れる（2634）。

【 0 0 1 1 】

次に、消費者2605は、購入したチケット2616のイベント会場2623へ行き、係員2622に、チケット2616を渡す（2632）。係員2622は、チケットの内容を目で確認し、チケットの内容が正しい場合に、消費者2605に入場を許可する（2633）。

【 0 0 1 2 】

また、有料放送を視聴するには、まず、ユーザは、放送業者と契約を結ぶ。放送番組と放送番組をデコードするための鍵情報は、放送局から送信され、専用の受信機で受信する。ユーザが番組を視聴するには、受信した鍵情報を用いて放送番組のスクランブルをデコードして、テレビ画面に表示する。有料放送を視聴した場合に課金処理が生じ、受信機に挿入されたＩＣカードに課金情報が書き込まれる。課金情報は、契約に基づき、定期的に放送業者に送信され、精算処理が行われる。

【 0 0 1 3 】

【発明が解決しようとする課題】

しかしながら、従来のチケットの販売システムでは、チケットを購入するには、結局、チケット販売店に行く必要があり、不便であった。

また、電子財布には、電子バリューを蓄積していくとメモリが不足するという問題があった。

また、従来の有料放送システムでは、放送事業者が、放送番組と番組のスクランブルをデコードする鍵情報を管理していた。

また、従来のプリペイドカードを用いた、前払い方式による決済システムでは、販売店が主導的に決済処理の作業を進めるので、販売店が消費者をだまして、

実際の商品の価格よりも、高い金額での決済処理を行なう場合があった。

【 0 0 1 4 】

また、従来の決済システムでは、販売店が、プリペイドカード端末を改造して、キャッシュレジスタの表示や、計算書の印字よりも、実際には、高い金額で決済処理を行なう場合があった。

また、従来の決済システムでは、基本的に、プリペイドカード端末によって、プリペイドカードの残高情報が書き換えられているだけであり、販売店が、プリペイドカード端末を改造して、実際にプリペイドカードから差引いた金額よりも高い金額を、センターシステムに請求する場合があった。

また、従来の決済システムでは、販売店に設置されているプリペイドカード端末に、直接、プリペイドカードをセットするので、販売店が、プリペイドカード端末を改造して、カード内の情報を改ざん、あるいは、プリペイドカード情報以外の個人情報を、不正に読み出す場合があった。

また、これらのプリペイドカード端末の不正な改造を防ぐために、分解ができないように、端末を封印するなど、物理的な対策を講ずる必要があり、このことが、プリペイドカード端末のコンパクト化と、コストダウンとのネックになっていた。

また、従来の決済システムでは、プリペイドカードの記録容量が限られており、また、プリペイドカードから差引かれた金額を、消費者が、直接、確認することができないことから、販売店は、決済時に、商品代金の明細とプリペイドカードの残高を印字した計算書を、消費者に手渡す必要があり、このことが、販売の効率化と、省資源の実現のネックになっていた。

【 0 0 1 5 】

また、従来のチケットの販売システムでは、チケットの改札を、人の目視によって行なうため、不正確であり、また、非効率的であった。この為、チケットの偽造等による不正が行なわれる場合があった。

また、従来の通信を用いた有料サービスの支払は、その都度口座振り込みを行うか、クレジットカードを指定する必要があった。

また、従来の有料放送サービスの支払は、放送事業者と事前に契約を結び、こ

の契約に基づいて口座引き落としまたはクレジットカード決済を行う方法に限定されていた。

また、従来の有料放送サービスでは、課金情報や履歴情報を受信側に蓄積し、この情報を定期的に収集するための通信回線を保持する必要があった。

【 0 0 1 6 】

本発明は、こうした従来の決済システムの課題を解決するもので、安全性と利便性とに優れたモバイル・エレクトロニックコマース・システムを提供することを目的としている。

【 0 0 1 7 】

【課題を解決するための手段】

これらの課題を解決するために本発明は、第 1 に、

無線通信手段を有する電子財布から、前記無線通信手段を通じて、必要な対価を支払い、供給側から商品やサービスの提供または必要な許可を受けるモバイル・エレクトロニックコマース・システムにおいて、

サービス提供手段が、指示閲覧手段から受信した購入要求に基づいて、電子的な有価カードのプログラムである電子バリューを、無線通信によって電子財布にインストールようにしたものである。

サービス提供手段は電子バリューの販売サーバ、指示閲覧手段はインターネットテレビやホームパソコンなどのホーム端末、電子財布は携帯端末を想定できる。

【 0 0 1 8 】

これにより、わざわざプリペイドカード販売店やチケット販売店に行かなくても、指示閲覧手段を用いて申込情報をサービス提供手段に送信することにより、ユーザは家庭や職場にしながら、電子プリペイドカードや電子チケットといった電子バリューを入手することができ、利便性が向上する。

また、ホーム端末を指示閲覧手段として利用することにより、電子財布よりも、大きな画面をみながら、購入する電子バリューを選択することができる。

【 0 0 1 9 】

第 2 に、

サービス提供手段が、発行した電子バリューを、電子バリューごとに設定された日時に、電子財布にインストールものであり、

これにより、電子バリューが有効になる期日直前に電子バリューを自動的に送信するといったことができ、使用しない電子バリューを電子財布に格納しないことで、電子財布のメモリの使用効率が向上する。

【0 0 2 0】

第3に、

サービス提供手段が、前記電子財布による対価の支払と電子バリューの未領収を証明する引換証を電子財布に発行するものであり、

この引換証により、電子バリューに対する支払を確認（ユーザは支払いと電子バリューの未領収を証明）することができ、取引の信頼性が向上する。

【0 0 2 1】

第4に、

供給側が、放送の復号化処理に用いる鍵情報を指示閲覧手段に提供するものであり、

これにより、従来の有料放送システムに限らず、モバイル・エレクトロニックコマース・システムにおいても、放送の復号化処理に用いる鍵情報の売買が可能となり、有料放送の提供方法の選択肢が増える。

【0 0 2 2】

第5に、

電子財布が、無線通信で、引換証に対応する電子バリューのインストールを所定の機関に要求するものであり、

これにより、電子財布の所有者の必要なときに、電子バリューをダウンロードでき、利便性が向上する。

【0 0 2 3】

第6に、

電子財布が、供給側へ対価を支払う手順の中に、次に示す手順が1つ以上含まれることを特徴とするものである。つまり、

(1)対価の支払いを申し出るメッセージを前記供給側へ送信。

- (2)前記供給側から、対価の支払いを請求するメッセージを受信。
- (3)前記供給側への対価の支払いを証明するメッセージを前記供給側へ送信。
- (4)前記供給側から、前記電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを受信。
- (5)前記レシートメッセージを受領したことを証明するメッセージを前記供給側へ送信。

【 0 0 2 4 】

これにより、電子バリュー決済手段は、電子財布と電子バリューの正当性を確認し、電子財布は、電子バリュー決済手段の正当性を確認できる。また、電子バリュー決済手段と電子財布は、実行された決済の正当性を確認でき、安全性が向上する。

また、正当性の確認を目視で行う必要がないため、間違いを防ぎ、手間が軽減される。

【 0 0 2 5 】

第 7 に、

電子財布が、第 6 の手段で示した手順を用い、指示閲覧手段を介して供給側へ対価を支払うものであり、

これにより、第 6 の手段を用いて対価の支払を行う電子財布は、新たに電子バリュー決済手段と直接通信回線を接続する必要なく、通信コストを削減できる。

【 0 0 2 6 】

第 8 に、

電子財布が、取引の識別情報を入力する入力手段を有し、前記入力手段で入力された識別情報を供給側に送信するものであり、

これにより、取引の一意性が保証され、取引の安全性が向上する。

【 0 0 2 7 】

第 9 に、

第 8 の手段で示した入力手段が、無線通信によって指示閲覧手段から取引の識別情報を取得する手段であるものであり、

これにより、入力の手間が省け、また、誤入力がなくなり、利便性が向上する

【0028】

第10に、

指示閲覧手段に提供されるサービスの対価を、電子財布に格納された電子バリューにより供給側に支払うものであり、

これにより、電子財布を用いて、指示閲覧手段に提供される有料サービスの代金を支払うことができ、利便性が向上する。

【0029】

第11に、

指示閲覧手段に提供されるサービスの対価を、前記指示閲覧手段に格納された履歴情報に基づいて、電子財布に格納された電子バリューにより供給側に支払うものであり、

これにより、電子財布を用いて、指示閲覧手段に提供された有料サービスの代金を支払うことができ、利便性が向上する。

【0030】

第12に、

電子財布が、指示閲覧手段から、前記指示閲覧手段に格納された履歴情報を受信し、受信した履歴情報を、供給側に送信するものであり、

これにより、提供側は、指示閲覧手段に提供側に情報送信するための通信回線を持たなくても、提供されたサービスの履歴を取得することができ、効果的なサービスを提供することができる。

【0031】

第13に、

電子財布が、指示閲覧手段に、提供側から受信した支払処理の結果を送信するものであり、

これにより、指示閲覧手段は、最新の支払結果に基づいて、課金プログラムを作動できる。

【0032】

第14に、

指示閲覧手段が、提供されたサービスの対価の支払を、無線通信で電子財布に要求するものであり、

これにより、指示閲覧手段は、対価の支払を行う手段を持たなくても、有料サービスの提供が受けられるようになる。

【0 0 3 3】

第 1 5 に、

指示閲覧手段が、通信手段を介して、供給側にサービスを要求し、供給側に対するサービスの対価の支払は、指示閲覧手段の無線通信手段を介して電子財布に要求するものであり、

これにより、提供を受ける指示閲覧手段を用いて、提供を受ける有料サービスを選択し、その支払を無線通信で接続された電子財布で行えるようになり、利便性が向上する。

【0 0 3 4】

第 1 6 に、

指示閲覧手段が、通信手段を介して供給側からチャンネル鍵を取得し、チャンネル鍵を用いてスクランブル鍵にかけられた暗号を解除し、復号化されたスクランブル鍵を用いて放送のスクランブルを解除するものであり、

これにより、従来放送を介して送信されていたチャンネル鍵が、ネットワークを介して入手できるようになり、有料放送の視聴方法の選択肢が増える。

【0 0 3 5】

第 1 7 に、

指示閲覧手段が、I C カード読み書き手段を有し、チャンネル鍵の格納とスクランブル鍵復号を、装着された I C カード上で行うものであり、

これにより、スクランブルの復号化に関する情報の安全性が向上する。

【0 0 3 6】

第 1 8 に、

指示閲覧手段が、提供されたサービスの履歴を格納した履歴情報に基づいて、電子財布に、対価の支払を要求するものであり、

これにより、提供されたサービスの対価を、まとめて後払いすることができ、

利便性が向上する。

【0037】

第19に、

指示閲覧手段が、支払処理結果を受信し、受信した処理結果に基づいて、履歴情報を変更するものであり、

これにより、第18の手段を用いて、支払を行う指示閲覧手段は、常に最新の履歴情報に基づき、課金処理を正確に行うことができる。

【0038】

【発明の実施の形態】

以下、本発明の各実施の形態について図面を用いながら説明する。なお、本発明はそれら実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

【0039】

(実施の形態1)

本発明の第1の実施の形態について、図1から図22を用いて説明する。

本発明の具体的な実施形態であるモバイル・エレクトロニックコマース・システムは、個人消費者が、ネットワークを介して、各種のチケットや、プリペイドカードを電子情報として購入し、チケットの改札や、一般の小売販売店で商品を購入、さらには、オンライン上の販売店で商品やサービスを購入する際に、係員に対してチケットを提示したり、店員との間で、直接、現金やレシートを受け渡したり、煩雑なクレジットカード決済の操作をする必要が無く、全て、無線通信によって、チケットの改札、商品やサービスの売買決済を行なうシステムである。

【0040】

以下では、電子情報化されたチケットやプリペイドカードを、総称して電子バリューと呼び、また、このシステムをモバイル・エレクトロニックコマース・システムと呼び、更に、このシステムによって提供される各種のサービスを、総称して、モバイル・エレクトロニックコマース・サービスと呼ぶこととする。

【0041】

このモバイル・エレクトロニックコマース・システムは、図1のシステム構成図に示すように、赤外線通信とデジタル無線電話通信との2系統の双方向無線通信機能と、電子バリュー購入機能と電子バリュー使用機能とを持つモバイルユーザ端末100と、

赤外線通信とデジタル電話通信との2系統の双方向通信機能を持ち、電子バリューの自動使用処理を行なうゲート端末101と、

オンラインサービスの提供と電子バリューによる決済処理を行なうコンテンツサーバ102と、

赤外線通信とデジタル電話通信との2系統の双方向通信機能とテレビ受信機能を持ち、テレビ放送の受信、オンライン上の情報の閲覧、コンテンツサーバからのサービス提供を受けるホーム端末103と、

クレジットサービス会社または決済処理会社におけるクレジット決済処理を行なう決済処理システム105と、

イベント会社またはチケット発行会社、小売販売会社、プリペイドカード発行会社における電子バリューの発行処理を行なう電子バリュー発行システム106と、

モバイルユーザ端末100とゲート端末101とコンテンツサーバ102とホーム端末103と決済処理システム105と電子バリュー発行システム106とを結ぶ通信ネットワークの中心に位置してモバイル・エレクトロニックコマース・サービスを提供するモバイルECサーバ104と、ネットワークにおけるデータ伝送路を提供するデジタル公衆網108と、モバイルユーザ端末100をデジタル公衆網108に接続する無線電話の基地局107とを備えている。

【0042】

図1において、109は、モバイルユーザ端末100と基地局107との間で行なうデジタル無線電話通信の伝送路を示し、112は、基地局112とデジタル公衆網108とを結ぶデジタル通信回線、110は、モバイルユーザ端末100とゲート端末101との間で行なう赤外線通信の伝送路、113は、ゲート端末101とデジタル公衆網108とを結ぶデジタル電話通信回線、111は、モバイルユーザ端末100とホーム端末103との間で行なう赤外線通信の伝送路、115は、ホーム端末103とデジタル公衆網10

8とを結ぶデジタル電話通信回線、116は、デジタル公衆網108とモバイルE Cサーバ104とを結ぶデジタル通信回線、114は、デジタル公衆網108とコンテンツサーバ102とを結ぶデジタル通信回線、117は、モバイルE Cサーバ104と決済処理システム105とを結ぶデジタル通信回線、118は、モバイルE Cサーバ104と電子バリュー発行システム106とを結ぶデジタル通信回線を示している。

【 0 0 4 3 】

また、モバイル・エレクトロニックコマース・サービスの通常の運用形態としては、次のような形態を想定している。

決済処理システム105は、クレジットカード会社または銀行または決済処理会社に設置され、電子バリュー発行システム106は、イベント会社またはチケット発行会社、小売販売会社、プリペイドカード発行会社に設置される。

さらに、ゲート端末101は、映画館やイベント会場等の入口に、コンテンツサーバ102は、オンライン上の販売店の運営会社に、ホーム端末103は、家庭や、ホテルの客室に設置され、モバイルユーザ端末100を、消費者が持ち歩く。

【 0 0 4 4 】

モバイルE Cサーバ104は、モバイル・エレクトロニックコマース・サービスを提供する会社に設置される。

さらに、モバイル・エレクトロニックコマース・システムを構成する各機器、および、各システムの所有者間の社会的な関係として、次のような関係を前提としている。

【 0 0 4 5 】

モバイルユーザ端末100の所有する消費者は、クレジットカード会社または銀行との間で、クレジットサービスの会員契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの会員契約を、さらに、無線電話通信会社との間では、無線電話通信サービスの契約を結んでいる。

【 0 0 4 6 】

ゲート端末101の所有者、例えば、映画館やイベント会場の経営者は、電子バリュー発行システム106の所有者との間で、電子バリュー発行システムが発行し

た電子バリューを取扱う契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの加盟店契約を、さらに、電話通信会社との間では、デジタル電話通信サービスの契約を結んでいる。但し、ゲート端末101の所有者と、電子バリュー発行システム106の所有者が、同一の所有者であっても良い。

【0047】

コンテンツサーバ102を所有する運営会社は、電子バリュー発行システム106の所有者との間で、電子バリュー発行システムが発行した電子バリューを取扱う契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの加盟店契約を、さらに、電話通信会社との間では、デジタル電話通信サービスの契約を結んでいる。但し、コンテンツサーバ102の所有者と、電子バリュー発行システム106の所有者が、同一の所有者であっても良い。また、コンテンツサーバ102が、有料放送の視聴権を販売する場合には、コンテンツサーバ102を所有する運営会社は、放送事業者との間で、有料放送の視聴権を発行する契約を結んでいる。但し、コンテンツサーバ102の所有者と、放送事業者が、同一の所有者であっても良い。

【0048】

電子バリュー発行システム106の所有者は、クレジットカード会社または銀行との間では、クレジットサービスの加盟店契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスのチケット発行者の契約を、さらに、通信事業会社との間では、デジタル通信サービスの契約を結んでいる。但し、電子バリュー発行システム106の所有者が、モバイル・エレクトロニックコマース・サービスを提供する会社であっても良い。

【0049】

また、決済処理会社が、決済処理システム105を用いてクレジット決済処理を行なう場合には、決済処理会社は、1社または複数のクレジットカード会社または銀行との間で、クレジット決済処理を決済処理会社が代行する契約を結んでいる。

【 0 0 5 0 】

なお、クレジットカードによって、クレジット決済処理を行う決済処理システムが異なる場合には、図 1 の決済処理システム 105 と同様の形態で、複数の決済処理システムが、モバイル EC サーバ 104 にデジタル通信回線によって接続される。

【 0 0 5 1 】

同様に、電子バリューの種類によって、電子バリュー発行システムが異なる場合には、図 1 の電子バリュー発行システム 106 と同様の形態で、複数のチケット発行システムが、モバイル EC サーバ 104 にデジタル通信回線によって接続される。

【 0 0 5 2 】

以下では、本システムの説明を簡単にするために、モバイルユーザ端末 100 の所有する消費者をユーザ (User)、ゲート端末 101 またはコンテンツサーバ 102 を所有し、商品やサービスを提供・販売する事業者をマーチャント (Merchant)、モバイル EC サーバ 104 を所有しモバイル・エレクトロニックコマース・サービスを提供する会社をサービス提供者 (Service Provider)、決済処理システム 105 を所有しクレジット決済処理を行なうクレジットカード会社または決済処理会社を決済処理機関 (Transaction Processor)、電子バリュー発行システム 106 を所有し電子バリューの販売を行なう事業者を電子バリュー発行者 (Electronic Value Issuer) と呼ぶこととする。

【 0 0 5 3 】

本システムによって提供されるモバイル・エレクトロニックコマース・サービスは、ネットワークを介した電子バリューの売買と、それにともなう電子バリューの配送と、その電子バリューの使用とを、全て電子的に行なうサービスである。

【 0 0 5 4 】

具体的には、ユーザがモバイルユーザ端末 100 を用いて、電子バリュー発行システム 106 から、モバイル EC サーバ 104 を介して電子バリューを購入し、モバイル EC サーバから、電子情報化されたチケットやプリペイドカードである電子バ

リユーを受信して、それをモバイルユーザ端末に蓄積して管理し、電子バリューを使用する際には、モバイルユーザ端末100とゲート端末101とのデータ通信によって、または、モバイルユーザ端末100とコンテンツサーバ102とのデータ通信によって、または、ホーム端末103を介したモバイルユーザ端末100とコンテンツサーバ102とのデータ通信によって、モバイルユーザ端末に蓄積されている電子バリューによる決済処理を行なうものである。

【 0 0 5 5 】

以上のサービスにおいて、本システムの各機器間で行われるデータ通信は、次に示す伝送路または通信回線を用いて行われる。

【 0 0 5 6 】

まず、モバイルユーザ端末100は、伝送路109、基地局107、デジタル通信回線112、デジタル公衆網108及びデジタル通信回線116を介して、モバイルECサーバ104とデジタル無線電話によるデジタル電話通信を行ない、また、伝送路109、基地局107、デジタル通信回線112、デジタル公衆網108及びデジタル通信回線114を介して、コンテンツサーバ102とデジタル無線電話によるデジタル電話通信を行ない、また、伝送路110を介してゲート端末101と赤外線通信を行ない、伝送路111を介してホーム端末103と赤外線通信を行なう。

【 0 0 5 7 】

ゲート端末101とモバイルECサーバ104とは、デジタル電話通信回線113、デジタル公衆網108及びデジタル通信回線116を介してデジタル電話通信を行なう。

コンテンツサーバ102とモバイルECサーバ104とは、デジタル通信回線114、デジタル公衆網108及びデジタル通信回線116を介してデジタルデータ通信を行なう。

ホーム端末103とモバイルECサーバ104とは、デジタル電話通信回線115、デジタル公衆網108及びデジタル通信回線116を介してデジタル電話通信を行ない、ホーム端末103とコンテンツサーバ102とは、デジタル電話通信回線115、デジタル公衆網108及びデジタル通信回線114を介してデジタル電話通信を行なう。

【 0 0 5 8 】

そして、モバイルECサーバ104と決済処理システム105とは、デジタル通信回

線117を介して、デジタルデータ通信を行ない、

モバイルECサーバ104と電子バリュー発行システム106とは、デジタル通信回線118を介して、モバイルECサーバ104とデジタルデータ通信を行なう。

【 0 0 5 9 】

また、モバイルユーザ端末100とモバイルECサーバ104との通信、及び、ゲート端末101とモバイルECサーバ104との通信、コンテンツサーバ101とモバイルECサーバ104との通信、さらに、モバイルECサーバ104と決済処理システム105との通信、モバイルECサーバ104と電子バリュー発行システム106との通信では、交換される情報を、全て、暗号化して通信する。暗号化には、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを組み合わせ、情報を電子封書化して通信する。

【 0 0 6 0 】

次に、本システムを構成する各構成要素について説明する。

ホーム端末103、ゲート端末101、コンテンツサーバ102、モバイルユーザ端末100、モバイルECサーバ104の順に説明する。

【 0 0 6 1 】

まず、ホーム端末103について説明する。

図2は、ホーム端末103の外観図であり、テレビモニタ202とアンテナ203をホーム端末103に接続した場合を示している。

【 0 0 6 2 】

図2において、204は、ユーザがホーム端末を操作するリモコン、201は、伝送路208を介してリモコン204と、伝送路111を介してモバイルユーザ端末100と、それぞれ赤外線通信を行なう赤外線通信モジュール、200は、電源スイッチであり、ホーム端末103は、映像ケーブル205と音声ケーブル206によってテレビモニタ202と、アンテナケーブル207によってアンテナ203と、それぞれ接続される。

【 0 0 6 3 】

ユーザは、リモコン204によってホーム端末を操作し、テレビ放送の視聴、オンライン上の情報の閲覧、コンテンツサーバ102からのオンラインサービスの提供を受ける。

コンテンツサーバ102から有料コンテンツを購入する場合には、ユーザは、モバイルユーザ端末100に格納された電子バリューによる決済処理を行なう。

【 0 0 6 4 】

決済処理には、有料コンテンツの種類により、コンテンツ提供毎の即時払い方式、課金情報を蓄積してまとめて決済を行う後払い方式、ホーム端末に電子バリューを蓄積しておき、決済を行う方式がある。コンテンツ提供毎の即時払い方式では、コンテンツサーバが、コンテンツ提供毎に、ユーザのモバイルユーザ端末から送信された電子バリューの認証を行い、領収書（レシート）を発行する。後払い方式、前払い方式では、コンテンツ提供に関する課金情報格納機能を利用し、蓄積した課金情報をもとに支払いを行う。

【 0 0 6 5 】

次に、ホーム端末103の内部の構成を説明する。

図3は、ホーム端末103のブロック構成図である。

ホーム端末103は、ROM(Read Only Memory)301に格納されたプログラムにしたがって、送信データと受信データの処理および他の構成要素の制御を行なうCPU(Central Processing Unit)300と、

CPU300が処理するデータ、および、CPU300が処理したデータが格納されるRAM(Random Access Memory)302と、

ユーザの加入者番号とスクランブル鍵およびチャネル鍵が格納されるEEPROM(Electric Erasable Programmable Read Only Memory)303と、

モバイルユーザ端末100およびリモコン207と赤外線通信を行なう赤外線通信モジュール201と、

テレビモニタ202に出力する映像信号と音声信号を生成する音声/映像処理部304と、

テレビ電波を受信したアンテナ203から供給されるテレビ信号をデコードし、選択されたチャンネルのビデオ信号309を生成するチューナ305と、

デジタル電話通信回線115との通信アダプタであるデジタル電話通信部306と、電源スイッチ200と、

CPU300が、赤外線通信モジュール201と音声/映像処理部304とチューナ305と

デジタル電話通信部306を制御する際のインターフェースの役割を果たす制御ロジック部307とを備えている。

なお、EEPROM(Electric Erasable Programmable Read Only Memory)303の代わりに、ICカードリーダーとICカードとを備えていても良い。

【 0 0 6 6 】

ROM301には、コンテンツサーバ102から受信した情報を閲覧するブラウザプログラムが格納されており、CPU300は、デジタル電話通信部306を介してコンテンツサーバ102から受信したデータから、表示データ信号308を生成する。

【 0 0 6 7 】

音声/映像処理部304は、CPU300の制御にしたがって、表示データ信号308とビデオ信号309を合成または切替えて、テレビモニタ202に出力する映像信号と音声信号を生成し、それぞれ、映像ケーブル205と音声ケーブル206に出力する。チューナ305がデコードするテレビ信号には、スクランブル鍵によるスクランブルがかけられている。スクランブル鍵は、さらにチャンネル鍵によって暗号化されて、放送局から定期的に、テレビ信号と共にホーム端末に送信され、EEPROM303に格納される。

【 0 0 6 8 】

チャンネル鍵は、チャンネル毎に異なり、ユーザと放送事業者との視聴契約およびユーザとマーチャントとの視聴権の売買契約に基づいて、放送局およびコンテンツサーバ102から提供され、EEPROM303に格納される。つまり、EEPROM303には、視聴が許されたチャンネルに対応するチャンネル鍵が格納される。EEPROM303の代わりに、ICカードリーダーとICカードとを備えている場合、スクランブル鍵とチャンネル鍵はICカードに格納される。

【 0 0 6 9 】

チューナ305は、CPU300の制御にしたがって、チャンネル鍵によって復号化されたスクランブル鍵を用いて、スクランブルがかけられたテレビ信号を復号化し、スクランブルが解除されたビデオ信号309を音声/映像処理部304に出力する。したがって、チャンネル鍵がない場合には、そのチャンネルを視聴することは出来ない。

【0070】

チャンネル鍵は、ホーム端末103とコンテンツサーバ102とのデジタル電話通信によって、コンテンツサーバ102が提供する商品やサービスを購入する場合と同様に、チャンネルの視聴権を購入することによって、チャンネル鍵がコンテンツサーバ102から提供され、EEPROM303またはICカードに格納される。また、放送局からホーム端末へのチャンネル鍵の提供は、ホーム端末がサポートする放送方式のチャンネル鍵の伝送方式に基づいて行われる。

【0071】

次に、ゲート端末101について説明する。ゲート端末に関しては、特許出願番号H09-0230564に詳しく述べられている。ここでは、図4を用いて、ゲート端末の概要を説明する。

【0072】

図4は、ゲート端末101の外観図である。図4において、400は、モバイルユーザ端末100と赤外線通信を行なう赤外線通信モジュール、401は、640×480画素表示のタッチパネル液晶ディスプレイ（タッチパネルLCD401）、402は、電源スイッチ、403は、テンキースイッチ、404は、タッチパネルLCD401の表示をメニュー画面に切替えるメニュースイッチ、405は、タッチパネルLCD401の表示及び、ゲート端末101への操作をロックさせるロックスイッチ、406は、赤外線モジュール400とゲート端末101本体とを接続するシリアルケーブルである。この他、ゲート端末101本体の背側面に、ゲート開閉装置等の外部装置を接続するRS-232Cインターフェイスがある。

【0073】

ゲート端末101の動作のモードには、大きく分けて、電子チケットを使用するチケット使用モードと、使用する電子チケットを設定する使用チケット設定モードの2つのモードがある。ゲート端末101の動作のモードは、画面をメニュー画面にして（メニュースイッチ405を押す）、タッチ操作によって、モードを選択することによって切替わる。

【0074】

チケット使用モードでは、ゲート端末101は、赤外線通信によって電子チケッ

トが提示されるのを待っている状態にあり、ユーザが、モバイルユーザ端末100を用いて電子チケットを提示する操作を行なうと、提示された電子チケットを検証し、モバイルユーザ端末100との間で使用処理情報を交換して、結果を画面に表示する。ゲート端末101のオペレータ（マーチャント）は、画面に表示される使用処理結果に基づいて、入場を許可、あるいは、入場を断ったりする。また、外部装置として、ゲート開閉装置をゲート端末101に接続すると、使用処理結果に基づいて、ゲートが開閉される。

【0075】

ロックスイッチ405は、オペレータ（マーチャント）がゲート端末101から離れる場合などに用いるスイッチであり、画面およびゲート端末101への操作をロックすることによって、ゲート端末101に対する不正な操作を防止する。ロックスイッチによって、一旦、ゲート端末101をロックすると、あらかじめ設定しておいたパスワードを入力するまで、ロックを解除することはできない。

【0076】

また、使用チケット設定モードでは、ゲート端末101に設定する電子チケットを指定するコード情報を、テンキースイッチ403で入力することで、サービス提供システム110から、指定された電子チケットを使用するプログラムモジュール（チケット使用モジュール）がダウンロードされ、使用する電子チケットが設定される。

【0077】

次に、コンテンツサーバ102について説明する。コンテンツサーバ102は、デジタル電話通信を行う通信装置を装備したパーソナルコンピュータによって構成される。

【0078】

図5は、コンテンツサーバ102のハードディスクに格納されるモバイル・エレクトロニックコマース・サービスに関するデータの模式図である。

設定情報などが格納されているサービスデータ領域500と、商品となるデジタルコンテンツデータを格納するコンテンツデータ領域501がある。

【0079】

サービスデータ領域500は、モバイル・エレクトロニックコマース・サービスにおける契約情報や、コンテンツサーバ102が取り扱う電子バリューに関する情報、および、電子バリュー使用の処理の履歴情報を格納する領域であり、この領域のデータは、モバイルECサーバ104に管理される。サービスデータ領域501には、マーチャント情報502、マーチャント公開鍵証明書503、マーチャント設定情報504、電話情報505、決済口座情報506、対象電子バリューリスト507、コンテンツリスト508、トランザクション履歴リスト509が格納されている。

【 0 0 8 0 】

マーチャント情報502は、マーチャントの名称、サービス提供者との契約内容等の情報、マーチャント公開鍵証明書503は、マーチャントの公開鍵証明書、マーチャント設定情報504は、モバイル・エレクトロニックコマース・サービスに関する、マーチャントの設定情報、電話情報505はマーチャントの電話番号、決済口座情報506はマーチャントが登録した決済の口座番号、対象電子バリューリスト507は、このコンテンツサーバ102が使用可能対象とする電子バリューのリスト情報、トランザクション履歴リスト509は、モバイル・エレクトロニックコマース・サービスでの電子バリュー使用の処理の履歴情報である。

【 0 0 8 1 】

コンテンツリスト508は、ユーザに提供されるコンテンツのリストで、コンテンツデータ領域501に格納されるデジタルコンテンツデータと対応している。例えば、コンテンツサーバ102が提供するサービスが、物品の販売の場合には、コンテンツリストには、販売する商品のリストが、コンテンツ領域には、商品のカタログ情報が格納される。また、画像データの販売の場合には、コンテンツリストには、管理している画像データのリストが格納され、コンテンツデータ領域501に、画像データが格納される。また、コンテンツサーバ102が提供するサービスが、有料放送の視聴権の販売の場合には、コンテンツリストには、管理しているチャンネル鍵のリストが、コンテンツデータ領域502にはチャンネル鍵のデータが格納される。

【 0 0 8 2 】

次に、モバイルユーザ端末100について説明する。

図6 (a)、(b)、(c)は、それぞれ、モバイルユーザ端末100の前面及び背面及び側面の外観図である。

【0083】

図6 (a)において、600は、ゲート端末101と赤外線通信を行なう赤外線通信ポート（赤外線通信モジュール）、601は、デジタル無線電話の電波を受発信するアンテナ、602は、レシーバスピーカ、603は、120×160画素表示のカラー液晶ディスプレイ（LCD）、604は、モバイルユーザ端末100の動作モードを切替えるモードスイッチ、605は、デジタル無線電話の通話スイッチ、606は、デジタル無線電話の終了スイッチ、607は、ファンクションスイッチ、608は、テンキースイッチ、609は、電源スイッチ、610は、マイクである。613は、端末内に格納されているID情報を赤外線通信で送信するボタン、ID送信ボタンである。

【0084】

さらに、図6 (b)において、611は、代金の支払や、トランザクションの内容の確認など、ユーザの確認をとまなう処理の実行を促す実行スイッチ、612は、ヘッドセットを接続するためのヘッドセットジャックである。

なお、図6 (c)に示すように、モバイルユーザ端末は、ICカードを挿入するICカードスロット614を備えていてもよい。

【0085】

モバイルユーザ端末100には、デジタル無線電話モードと、電子バリューモード、個人情報管理モード、ID送信モードの4つの動作モードがあり、モードスイッチ604によって切替わる。

【0086】

図6 (a)は、電子バリューモードの場合のLCD603に表示される画面を示している。

モバイルユーザ端末100は、デジタル無線電話モードでは、デジタル無線電話サービスを提供する通信事業者との契約に基づくデジタル無線電話として動作する。電子バリューモードは、モバイルユーザ端末100に格納された複数の電子バリューのLCD603への表示、および、モバイルユーザ端末に格納された電子バリューを、ゲート端末またはコンテンツサーバに対して使用する動作モード、個人情報

管理モードは、モバイルユーザ端末100の内部に格納されるユーザの個人情報を管理をする動作モードであり、個人情報管理モードにおいて、ユーザは、登録されている個人情報や写真データ等の参照、及び、ユーザ設定情報の設定を行う。ID送信モードは、モバイルユーザ端末100の内部に格納されるID情報を送信するモードである。

【0087】

このモバイルユーザ端末100を用いて、例えば、普通に電話をかける場合には、ユーザは、まず、モードスイッチ604で、動作モードをデジタル無線電話モードにし、次に、テンキースイッチ608で電話番号を入力して、通話スイッチ605を押す。以上の操作で、ユーザは、入力した電話番号に電話をかけることができる。

【0088】

また、モバイルユーザ端末100に通常の電話がかかって来た場合には、モバイルユーザ端末100は、その時の動作モードに関係なく、着信音を発する。この場合には、通話スイッチ605を押すことで自動的にデジタル無線電話モードに切り替わり、ユーザは電話を受けることができる。

【0089】

また、電子バリューを使用して改札を受ける場合には、まず、モードスイッチ604により動作モードを電子バリューモードに設定し、ファンクションスイッチ607（“F1”or“F2”）で、提示するチケットを選択する（使用する電子チケットをLCDに表示させる）。次に、赤外線通信ポート600を、映画館やイベント会場等の入口に設置されたゲート端末101の方向に向けて、実行スイッチ611を押す。以上の操作によって、モバイルユーザ端末100は、ゲート端末101との間で赤外線通信を行ない、チケットの使用処理情報を交換して、電子チケットの使用処理を行なうものである。

【0090】

また、コンテンツサーバに対して電子バリューを使用するには、まず、モードスイッチ604により動作モードを電子バリューモードに設定し、ファンクションスイッチ607（“F1”or“F2”）で、提示するチケットを選択する（使用する電子チ

ケットをLCDに表示させる)。次に、ホーム端末に表示された指示にしたがって、入力を行い、実行スイッチ611を押す。以上の操作によって、コンテンツサーバと無線電話通信を行い、チケットの使用の処理を行う。また、コンテンツサーバの種類によっては、使用する電子チケットをLCDに表示させて、実行スイッチ611を押すと、ホーム端末との間で赤外線通信を行なって、チケットの使用処理を行ったり、または、使用する電子チケットをLCDに表示させて、実行スイッチ611を押すと、ホーム端末との間で赤外線通信を行なった後、コンテンツサーバと無線電話通信を行い、チケットの使用の処理を行う。

【0091】

ID送信モードでは、ID送信ボタン613が有効となり、ID送信ボタン613を押すと、端末内に格納されているID情報を赤外線通信で送信する。また、モバイルユーザ端末がICカードスロット614を備え、それにICカードが挿入されている場合、ICカードに格納されているID情報を送信する。

【0092】

次に、モバイルユーザ端末100の内部の構成について説明する。

図7は、モバイルユーザ端末100に格納されるデータの模式図である。

モバイルユーザ端末100の内部のメモリには、基本プログラム領域700、サービスデータ領域701、ユーザ領域702、ワーク領域703、及びテンポラリ領域704の5つの領域がある。基本プログラム領域700は、モバイルユーザ端末100のROMに格納されているプログラムのバージョンアップされたモジュール、及び、パッチプログラムや、追加プログラムが格納される。

【0093】

ユーザ領域702は、ユーザが自由に使用できる領域、ワーク領域703は、モバイルユーザ端末100のCPUがプログラムを実行する際に使用する作業領域、また、テンポラリ領域704は、モバイルユーザ端末100が受信した情報を一時的に格納する領域である。サービスデータ領域は、モバイル・エレクトロニックコマース・サービスにおける契約情報や、電子バリュー情報、履歴情報などを格納する領域であり、この領域のデータは、モバイルECサーバ104によって管理される。

【0094】

サービスデータ領域701には、個人情報705、ユーザ公開鍵証明書706、ユーザ設定情報707、電話情報708、決済口座情報709、電子バリュースト710、使用履歴リスト711が格納されている。個人情報705は、ユーザの名前、年齢、性別等の情報、ユーザ公開鍵証明書706は、ユーザの公開鍵証明書、ユーザ設定情報707は、モバイル・エレクトロニックコマース・サービスに関する、ユーザの設定情報、電話情報708は、電話番号等のデジタル無線電話に関連する情報、決済口座情報709は、ユーザが登録した決済口座の情報、電子バリュースト710は、ユーザが所有する電子バリューストのリスト情報とそのデータの実体、使用履歴リスト711は、モバイル・エレクトロニックコマース・サービスの使用履歴情報である。

また、モバイルユーザ端末がICカードスロット614を備えている場合、上記のデータの一部またはすべてが、ICカードに格納される。

【 0 0 9 5 】

次に、モバイルECサーバ104について説明する。

モバイルECサーバ104は、モバイルユーザ端末100、ゲート端末101、コンテンツサーバ102、決済処理システム106、電子バリュー発行システム106と、それぞれ通信を行い、ユーザ、マーチャント、決済処理機関、電子バリュー発行者間の仲介をして、ユーザと、マーチャントに対して、モバイル・エレクトロニックコマース・サービスを提供するシステムである。

【 0 0 9 6 】

図8は、モバイルECサーバ104における処理のアーキテクチャを示している

モバイルECサーバ104は、モバイル・エレクトロニックコマース・サービスを、モバイルECサーバ104上のマーチャント処理部801、ユーザ処理部802、WWWサーバ803、決済処理部804、電子バリュー発行処理部805、司令部806の連携処理によって提供する。

図8において、ユーザ処理部802は、モバイルECサーバ104とモバイルユーザ端末100との通信のインターフェイスとなるプロセスである。

【 0 0 9 7 】

マーチャント処理部801は、モバイルECサーバ104と、ゲート端末101または

コンテンツサーバ102との通信のインターフェイスとなるプロセスである。

【0098】

決済処理部804は、モバイルECサーバ104と決済処理システム106との通信のインターフェイスとなり、電子バリュー発行処理部805は、モバイルECサーバ104と電子バリュー発行システム106との通信のインターフェイスとなるプロセスである。

【0099】

命令部806は、ユーザ処理部802、マーチャント処理部801、決済処理部804、電子バリュー発行処理部805、WWWサーバ803を管理し、それぞれと通信をして、モバイル・エレクトロニックコマース・サービスを実現するプロセスである。

【0100】

モバイルECサーバ104は、一台のコンピュータで構成される場合と複数台のコンピュータによって構成される場合がある。複数台のコンピュータによって構成される場合には、マーチャント処理部801、ユーザ処理部802、WWWサーバ803、決済処理部804、電子バリュー発行処理部805、命令部806は、各処理の負荷が分散されるように、複数台のコンピュータに分散して配置してもよい。

【0101】

まず、ユーザ処理部802について説明する。

ユーザ処理部802は、モバイルユーザ端末100の所有者（ユーザ）に関する情報の管理、モバイルユーザ端末100との通信制御と、ユーザの認証、モバイルユーザ端末100への送信データの暗号化、モバイルユーザ端末100からの受信データの復号化、モバイルユーザ端末100からの受信データの有効性のチェック、さらに、モバイルユーザ端末100との間で、リモートアクセスと、リモート処理によるデータアップデート、データバックアップの処理を行う。

【0102】

次に、マーチャント処理部801について説明する。

マーチャント処理部801は、マーチャントに関する情報の管理と、ゲート端末101またはコンテンツサーバ102との通信制御、マーチャントの認証、ゲート端末101またはコンテンツサーバ102への送信データの暗号化、ゲート端末101またはコ

ンテンツサーバ102からの受信データの復号化、ゲート端末101またはコンテンツサーバ102からの受信データの有効性のチェック、ゲート端末101またはコンテンツサーバ102との間で、リモートアクセスと、リモート処理によるデータアップデート、データバックアップの処理を行う。

【0103】

次に、決済処理部804について説明する。

決済処理部804は、決済処理システム106が設置されている決済処理機関に関する情報の管理と、決済処理システム106との通信制御、決済処理機関の認証、決済処理システム106への送信データの暗号化、決済処理システム106からの受信データの復号化、決済処理システム106からの受信データの有効性のチェックを行う。

【0104】

次に、電子バリュー発行処理部805について説明する。

電子バリュー発行処理部805は、電子バリュー発行者に関する情報の管理と、電子バリュー発行システム106との通信制御、電子バリュー発行者の認証、電子バリュー発行システム106への送信データの暗号化、電子バリュー発行システム106からの受信データの復号化、電子バリュー発行システム106からの受信データの有効性のチェックを行う。

【0105】

次に、司令部806について説明する。

司令部806は、モバイルECサーバ104内の、ユーザ処理部802、マーチャント処理部801、決済処理部804、電子バリュー発行処理部805、WWWサーバ803を管理し、それぞれと通信をして、モバイル・エレクトロニックコマース・サービスを実現するプロセスである。

【0106】

モバイルECサーバ104の処理は、大きく分けて2つある。1つは、ユーザに対する電子バリューの提供であり、もう一つは、ゲート端末101またはコンテンツサーバ102に対する電子バリューの精算である。司令部には、これらの処理のシーケンスが設定してあり、司令部は、この設定されたシーケンスにしたがって

、モバイルECサーバ104内の各処理部から送られるメッセージを処理し、また、各処理部に対して、処理を促すメッセージを送る。そして、各処理部は、それぞれ、司令部806から送られるメッセージに対応する処理を行う。このように、司令部806と、モバイルECサーバ104内の各処理部が連携して処理を行うことによって、モバイル・エレクトロニックコマース・サービスの処理が行われる。

【0107】

例えば、電子バリュー購入の処理の場合には、ユーザからの購入要求を、WWWサーバ803から受信した司令部806は、購入シーケンスにしたがって、まず、ユーザ処理部802でユーザの認証を行い、次に、決済処理部804で決済処理を行い、次に、電子バリュー発行処理部805で電子バリューの発行を行い、次に、生成した電子バリューをユーザ処理部802からユーザに送信し、WWWサーバ803に購入処理の終了を通知をする。購入処理については、あとで詳しく説明する。

【0108】

また、ゲート端末101またはコンテンツサーバ102の電子バリュー精算処理の場合には、司令部は、設定されたタイムスケジュールにしたがって、定期的にマーチャント処理部801でゲート端末101またはコンテンツサーバ102と通信を行い、まず、マーチャント処理部801から、ゲート端末101またはコンテンツサーバ102のトランザクション履歴リスト511を受信し、次に、受信した情報を基に、決済処理部804と必要な決済処理を行い、次に、マーチャント処理部801から、ゲート端末101またはコンテンツサーバ102に精算の結果を送信する。

【0109】

次に、モバイルECサーバ104のユーザ処理部802が管理する情報について説明する。

ユーザ処理部802は、ユーザの属性情報とユーザのモバイルユーザ端末100の内部のデータを管理する。

図9は、一人のユーザに対して、ユーザ処理部802に格納されるデータである。

【0110】

ユーザ処理部802では、一人のユーザに対して、ユーザ名900、ユーザID901、個人情報902、ユーザ公開鍵証明書903、端末情報904、ユーザ設定情報905、電話

情報906、決済口座情報907、電子バリューリスト908、及び使用履歴リスト909が管理される。

【0111】

個人情報902は、ユーザの年齢、生年月日、職業、契約内容等のユーザ個人に関する情報であり、この情報の一部が、モバイルユーザ端末100の個人情報705に対応している。

【0112】

ユーザ公開鍵証明書903は、ユーザの公開鍵証明書、端末情報904は、モバイルユーザ端末100の属性情報、ユーザ設定情報905は、モバイル・エレクトロニック・コマース・サービスに関する、ユーザの設定情報、電話情報906は、電話番号等のデジタル無線電話に関連する情報、決済口座情報907は、ユーザが登録した決済口座の情報、電子バリューリスト908は、ユーザが所有する電子バリューのリスト情報、使用履歴リスト909は、モバイル・エレクトロニック・コマース・サービスの使用履歴情報である。

【0113】

ユーザ設定情報905、電話情報906、決済口座情報907、電子バリューリスト908、及び使用履歴リスト909は、それぞれ、モバイルユーザ端末100のユーザ設定情報707、電話情報708、決済口座情報709、電子バリューリスト710、及び使用履歴リスト711に対応する情報である。

【0114】

次に、モバイルECサーバ104のマーチャント処理部801が管理する情報について説明する。

図10は、一つのゲート端末101またはコンテンツサーバ102に対して、マーチャント処理部801に格納される情報を示す。

【0115】

マーチャント処理部801では、一つのゲート端末101またはコンテンツサーバ102に対して、マーチャント名1000、マーチャントID1001、ゲート端末ID/コンテンツサーバID1002、マーチャント情報1003、公開鍵証明書1004、端末情報1005、マーチャント設定情報1006、電話情報1007、決済口座情報1008、対象電子バ

リユーリスト1009、トランザクション履歴リスト1010が管理される。また、コンテンツサーバ102に関する情報の場合には、これに加え、コンテンツリストも管理される。

【0116】

マーチャント情報1003は、マーチャントの住所、契約内容等のマーチャントまたは通信事業者に関する情報であり、この情報の一部が、ゲート端末101またはコンテンツサーバ102のマーチャント情報505に対応している。

【0117】

公開鍵証明書1004は、マーチャントの公開鍵証明書、端末情報1005は、ゲート端末101またはコンテンツサーバ102の属性情報、マーチャント設定情報1006は、モバイル・エレクトロニックコマース・サービスに関する、マーチャントの設定情報、電話情報1007は、デジタル電話、デジタル無線電話に関連する情報、決済口座情報1008は、マーチャントが精算するのに使用する口座情報、対象電子バリュースト1009は、マーチャントが使用可能対象とする電子バリューとして設定した電子バリューのリスト情報、トランザクション履歴リスト1010は、モバイル・エレクトロニックコマース・サービスでの履歴情報である。

【0118】

マーチャント設定情報1006、電話情報1007、決済口座情報1008、対象電子バリュースト1009、トランザクション履歴リスト1010は、それぞれ、ゲート端末101またはコンテンツサーバ102のマーチャント設定情報507、電話情報508、決済口座、対象電子バリュースト510、トランザクション履歴リスト511に対応する情報である。

コンテンツリストは、コンテンツサーバで管理されているデジタルコンテンツデータのリストであり、コンテンツサーバ102のコンテンツリスト508に対応している。

【0119】

図11は、一つの決済処理機関に対して、決済処理部804に格納される情報を表した模式図である。

決済処理部804では、一つの決済処理機関に対して、1100決済処理機関名、110

1 決済処理機関 I D、1102 決済処理機関情報、1103 決済処理機関公開鍵証明書、及び決済履歴リスト 1104 を管理する。

【 0 1 2 0 】

決済処理機関情報 1102 は、決済処理機関の住所、契約内容等の決済処理機関に関する情報であり、決済処理機関公開鍵証明書 1103 は、決済処理機関の公開鍵証明書、決済履歴リスト 1104 は、モバイル・エレクトロニックコマース・サービスでのクレジットカード決済の履歴情報である。

【 0 1 2 1 】

次に、モバイル E C サーバ 104 の電子バリュー発行処理部 805 が管理する情報について説明する。

電子バリュー発行処理部 805 は、電子バリュー発行者の属性情報とその電子バリュー発行者による電子バリュー発行の履歴情報を管理する。

【 0 1 2 2 】

図 1 2 は、一つの電子バリュー発行者に対して、電子バリュー発行処理部 805 に格納される情報を示している。

電子バリュー発行処理部 805 では、一つの電子バリュー発行者に対して、電子バリュー発行者名 1200、電子バリュー発行者 I D 1201、電子バリュー発行者情報 1202、電子バリュー発行者公開鍵証明書 1203、サービスコードリスト 1204、トランザクション履歴リスト 1205 が管理される。

【 0 1 2 3 】

電子バリュー発行者情報 1202 は、電子バリュー発行者の住所、契約内容等の電子バリュー発行者に関する情報、電子バリュー発行者公開鍵証明書 1203 は、電子バリュー発行者の公開鍵証明書、サービスコードリスト 1204 は、電子バリュー発行者が提供するサービスの種類を示すサービスコードのリスト、トランザクション履歴リスト 1205 は、電子バリュー発行者による電子バリュー発行の履歴情報である。

【 0 1 2 4 】

次に、モバイル E C サーバ 104 の司令部 806 に格納される情報について説明する

図 1 3 は、司令部806に格納される情報を示している。

司令部806には、ユーザリスト1300、マーチャントリスト1301、決済処理機関リスト1302、電子バリュー発行者リスト1303、WWWサーバ情報1304、サービス提供履歴リスト1305、電子バリュー管理情報1306が管理される。

【 0 1 2 5 】

ユーザリスト1300は、サービス提供者と契約をしているモバイルユーザ端末100の属性情報のリスト、マーチャントリスト1301は、サービス提供者と契約をしているゲート端末101の属性情報のリスト、決済処理機関リスト1302は、サービス提供者と契約をしている全決済処理機関の属性情報のリスト、電子バリュー発行者リスト1303は、サービス提供者と契約をしている全電子バリュー発行者の属性情報のリスト、サービス提供履歴リスト1305は、モバイル E C サーバ104が提供したモバイル・エレクトロニック・コマース・サービスの履歴情報のリスト、電子バリュー管理情報1306は、発行された電子バリューの管理情報である。

【 0 1 2 6 】

次に、本発明のモバイル・エレクトロニック・コマースで流通する、電子バリューのデータ構造について説明する。

図 1 4 は、電子バリューのデータ構造を示す模式図である。ここで、二重線で囲まれた部分は、デジタル署名が施されている部分を示す。図 1 4 において、一つの電子バリュー1400は、電子バリュープログラム1401、提示電子バリュー1402、電子バリュー証明書1403の三つの部分から構成される。電子バリュープログラム1401は、電子バリューのステータスの管理、及び、電子バリュー固有の動作を規定する情報であり、提示電子バリューは、電子バリューを使用する際に、電子バリューの内容を示す情報として、ゲート端末101（またはコンテンツサーバ102）に提示する情報であり、電子バリュー証明書1403は、サービス提供者が発行する電子バリューの証明書であり、電子バリューが本物であることを示す情報である。

【 0 1 2 7 】

一つ電子バリュー1400は、公開鍵暗号方式の3種類、4つの鍵を持つ。1種類は、電子バリューのデジタル署名用の鍵であり、秘密鍵と、それに対応する公開鍵

として、それぞれ、電子バリュープログラム1401に格納されている電子バリュー署名秘密鍵1406と、電子バリュー証明書1403に格納されている電子バリュー署名公開鍵である。もう1種類は、ゲート端末101（またはコンテンツサーバ102）との間での電子バリューの認証処理に用いる、電子バリュープログラム1401に格納されている電子バリュー認証秘密鍵1407であり、もう1種類は、モバイルユーザ端末100側でのゲート端末101またはコンテンツサーバ102の認証処理に用いる、電子バリュープログラム1401に格納されているトランザクション端末認証公開鍵1408である。

【0128】

電子バリュー署名秘密鍵1406と電子バリュー署名公開鍵は、一つ一つの電子バリューごとに異なる鍵対であり、電子バリュー認証秘密鍵1407と、トランザクション端末認証公開鍵1408は、電子バリューの種類ごとに異なる鍵である。ゲート端末101には、電子バリュー認証秘密鍵1407とトランザクション端末認証公開鍵1408にそれぞれ対応する電子バリュー認証公開鍵と、トランザクション端末認証秘密鍵とが設定されている。

【0129】

図14において、まず、電子バリュープログラム1401は、電子バリューステータス1404、電子バリュープロパティ1405、電子バリュー署名秘密鍵1406、電子バリュー認証秘密鍵1407、トランザクション端末認証公開鍵1408、電子バリュープログラムデータによって構成される。

【0130】

電子バリューステータス1404は、電子バリューの状態（ステータス）を示す情報であり、電子バリューの使用の可否等を示す情報である。

電子バリュープロパティ1405は、電子バリューの種類によって、オプションで設定される情報である。例えば、電子バリューが回数券の場合、ここには、回数券の初期値と使用回数が設定される。使用回数は、使用される毎に、1ずつインクリメントされる。また、電子プリペイドカードの場合、ここには、プリペイドカードの金額の初期値と使用済額が設定される。使用済額は、使用されるたびに、使用された値が加算される。

【 0 1 3 1 】

電子バリュー署名秘密鍵1406は、前述した電子バリューのデジタル署名用の秘密鍵であり、同様に、電子バリュー認証秘密鍵1407は、電子バリューの認証処理に用いる秘密鍵、トランザクション端末認証公開鍵1408は、ゲート端末101（またはコンテンツサーバ102）の認証処理に用いる公開鍵である。

【 0 1 3 2 】

電子バリュープログラムデータ1409は、その電子バリュー固有の動作を規定するプログラムモジュールであり、この電子バリュープログラムデータと電子バリュープロパティ1405との組み合わせによって、いろいろな種類の電子バリューが規定でき、電子バリュー使用の処理における各種の動作を規定することができる。

【 0 1 3 3 】

次に、提示電子バリュー1402は、電子バリューコード1410、電子バリュー I D 1411、電子バリュー情報1412、電子バリュー発行者 I D 1413、サービス提供者 I D 1414の情報によって構成される。電子バリュー I D 1411と電子バリュー情報1412と電子バリュー発行者 I D 1413には、電子バリュー発行者によるデジタル署名が施され(1416)、提示電子バリュー1402としては、サービス提供者によるデジタル署名が施されている(1415)。

【 0 1 3 4 】

電子バリューコード1410は、電子バリューの種類を示すコード情報である。電子バリュー I D 1411は、一つ一つの電子バリューごとに異なる識別情報である。

電子バリュー情報1412は、電子バリューの内容を示す A S C I I 情報であり、電子バリューのタイトルや、日時、場所、席種、主催者、さらには、電子バリューの譲渡の可否や、回数券として動作する場合には、回数券の枚数等の使用条件情報が、それぞれの情報の種類を示すタグ情報を付加した形式で記述されている。

【 0 1 3 5 】

電子バリュー発行者 I D 1413は、この電子バリューを発行した電子バリュー発行者を示す I D 情報であり、サービス提供者 I D 1414はサービス提供者を示す I

D情報である。

電子バリュー証明書1403は、電子バリューID、電子バリュー署名公開鍵、電子バリュー証明書ID、サービス提供者ID、電子バリュー証明書発行日時によって構成され、サービス提供者のデジタル署名が施されている(1415)。

【0136】

次に、本発明における、モバイル・エレクトロニックコマース・システムで提供されるモバイル・エレクトロニックコマース・サービスについて説明する。

モバイル・エレクトロニックコマース・サービスには、ユーザとモバイルECサーバが行う電子バリューの購入と、ユーザとゲート端末（またはコンテンツサーバ）が行う電子バリューの使用と、ゲート端末（またはコンテンツサーバ）とモバイルECサーバが行う精算がある（。なお「電子バリューの購入」に関しては、図15～17に電子バリュー発行処理部と電子バリュー発行システム、決済処理部、決済処理システムを参照）。

【0137】

電子バリューの購入は、ユーザ1500が、電子バリュー発行者に電子バリューの申込を行い、電子バリューを購入する処理であり、電子バリューの使用は、ユーザ1500が電子バリューを使用して、ゲート端末101（またはコンテンツサーバ102）からのサービス提供を受ける処理である。

【0138】

まず、電子バリューの購入の処理を説明し、次に、電子バリューの使用を説明する。

まず、図15～19を用いて、電子バリューの購入の処理を説明する。

図15～17は、インターネットを使用した電子バリュー購入処理の手順を示し、図18(a)(b)は、電子バリュー購入時のテレビモニタ202の画面表示の例を示し、図18(c)(d)(e)は、電子バリュー購入時のモバイルユーザ端末のLCDの画面表示の例を示し、図19は、電子バリュー購入時のメッセージのデータ構造を示している。図19で、太線で囲まれた部分は、封書化されている部分を示し、二重線で囲まれた部分は、デジタル署名が施されている部分を示し、太二重線で囲まれた部分は、ハッシュ演算して、暗号化されている部分を

示す。

【0139】

図15に示すように、まず、ユーザ1500は、ホーム端末103からデジタル公衆網108を介してWWWサーバ803に接続し、電子バリューのオーダー画面を表示する。ユーザは、図18(a)に示すように、リモコン204を操作して、テレビモニタに表示されたオーダー画面で、購入する電子バリューを選択し、注文ボタンを選択する(オーダー操作1501)。

【0140】

ユーザがオーダー操作1501を行うと、ホーム端末103は、購入を申し込むメッセージ、オーダー情報1502を、WWWサーバ803に送信する。オーダー情報には、オーダーされた電子バリューを識別する情報が含まれている。オーダー情報1502を受信したWWWサーバ803は、オーダー情報1502を司令部806に送信する。オーダー情報1502を受信した司令部806は、オーダーされた電子バリューに対する情報を要求するメッセージ、オファー要求1503を電子バリュー発行処理部805に送信する。オファー要求1503には、オーダーされた電子バリューを識別する情報が含まれている。オファー要求1503を受信した電子バリュー発行処理部805は、オーダーされた電子バリューを発行する電子バリュー発行システムに、オーダーされた電子バリューに関する情報、電子バリュー販売オファーを要求するメッセージ、販売オファー要求1504を送信する。販売オファー要求1504を受信した電子バリュー発行システムは、要求された電子バリューに対する電子バリュー販売オファー1505を生成し、電子バリュー発行処理部805に送信する。電子バリュー発行処理部805は、受信した電子バリュー販売オファー1505を、司令部に送信する。

【0141】

ユーザ1500が希望する電子バリューが発行可能な場合、電子バリュー販売オファー1505には、発行可能な電子バリューの席番号や、電子バリューの代金を示す情報が含まれ、売切れ等で、電子バリューが発行できない場合には、情報は含まれない。

【0142】

電子バリュー販売オファー1505を受信した司令部は、オーダー情報1502に応答

するメッセージ、オファー情報1506を、WWWサーバ803に送信する。オファー情報1506には、電子バリュー販売オファーが含まれる。オファー情報1506を受信したWWWサーバは、受信したオファー情報1506を、ホーム端末103に送信する。

【0143】

オファー情報1506を受信したホーム端末103は、電子バリュー販売オファーをユーザ1500に表示する（オファー表示1507）。この時、オファー情報1506に、電子バリュー販売オファーが含まれている場合、テレビモニタには、図18（b）に示すように、電子バリュー販売オファーが表示され、電子バリュー販売オファーが含まれていない場合には、電子バリューが発行できない旨を示すメッセージが表示される。

【0144】

図18（b）に示すように、オファー表示1507には、ユーザIDを入力するエントリと、“購入”と“キャンセル”の2つの操作メニューがある。リモコン204で“キャンセル”を選択すると、その電子バリュー販売オファーはキャンセルされる。また、リモコン204で、一文字ずつユーザIDを入力して、“購入”を選択すると（購入操作1508）、ホーム端末103は、ユーザ1500がWWWサーバに電子バリューの購入を要求するメッセージ、購入情報1509を生成し、WWWサーバ803に送信する。購入情報1509には、ユーザIDと、ユーザが購入する電子バリューの識別情報が含まれる。

【0145】

この時、このユーザID入力において、ユーザがリモコン204を操作して、一文字ずつユーザIDを入力する代わりに、モバイルユーザ端末100を用いて、ユーザIDをホーム端末103に送信することもできる。この場合、ユーザは、まず、モバイルユーザ端末100をID送信モードにし、赤外線通信ポート600をホーム端末の赤外線通信モジュールに向け、ID送信ボタン613を押す。すると、モバイルユーザ端末に格納されているユーザIDが赤外線通信によってホーム端末に送信され、ホーム端末103は、受信したユーザIDをテレビモニタ上に表示する。

【0146】

購入情報1509を、受信したWWWサーバ803は、オファー情報1506に基づいて、購

入を申し込むメッセージ、購入要求1509を生成し、モバイルECサーバ104の司令部806に送信する。購入要求1509を受信した司令部806は、購入要求1509に基づいて、ユーザ処理部に購入の認証処理を要求するメッセージ、購入認証要求1510を生成し、ユーザ処理部に送信する。購入認証要求1510には、ユーザIDと、ユーザが購入する電子バリューの識別情報が含まれており、購入認証要求1510を受信したユーザ処理部は、ユーザIDに対応するユーザ1500のユーザ公開鍵証明書903と電話情報906とから、それぞれ、ユーザ1500の公開鍵とモバイルユーザ端末100の電話番号を取得し、さらに、購入のための認証を行う乱数 (Rand) 170を生成して、ユーザに購入の認証処理を要求するメッセージ、認証情報要求1511を生成し、デジタル電話通信で、モバイルユーザ端末100に送信する。図19 (a) に示すように、認証情報要求1511には、それが認証情報要求1511であることを示すメッセージID1700と、乱数 (Rand) 1701をユーザ1500の公開鍵で封書化したデータ1702が含まれる。

【0147】

認証情報要求1511を受信したモバイルユーザ端末100は、ユーザ1500の秘密鍵で封書を解き、乱数 (Rand) 1701を求め、図18 (c) に示すように、ユーザ1500に購入実行の確認を促す画面を表示する (認証要求表示1512)。

【0148】

ユーザ1500が、実行スイッチ311を押すと (購入確認操作1513)、モバイルユーザ端末100は、認証要求メッセージの応答をするメッセージ、認証情報応答1514を、モバイルECサーバ104のユーザ処理部802に送信する。認証情報応答1514は、図19 (b) に示すように、それが認証情報応答1514であることを示すメッセージID1703と、モバイルユーザ端末100が任意に生成した要求番号1704と、復号化した乱数1705を、モバイルECサーバ104の公開鍵で封書化したデータ1706を含む。

【0149】

認証情報応答1514を受信したモバイルECサーバ104のユーザ処理部802は、受信した認証情報応答を、モバイルECサーバ104の秘密鍵で復号化して得た乱数 (Rand) と、送信した乱数 (Rand) 1701を照合して、有効性を検証し、司令部80

6に、認証結果を通知するメッセージ、購入認証結果1515を送る。乱数が一致した場合、モバイルECサーバ104の司令部806は、電子バリュー発行処理部805に、電子バリューを申し込むメッセージ、電子バリュー購入1516を送信する。電子バリュー購入1516には、購入するバリューのサービスコードが含まれる。電子バリュー購入1516を受信した電子バリュー発行処理部805は、サービスコードに対応した電子バリュー発行者に対して、電子バリューの購入を申し込むメッセージ、電子バリュー購入申込1517を生成し、電子バリュー発行システム106へ送信する。

【0150】

電子バリュー購入申込1517を受信した電子バリュー発行システム106は、申込まれた電子バリューの電子バリューデータを生成する。電子バリューデータとは、電子バリューID1411と電子バリュー情報1412と電子バリュー発行者ID1413とからなるデータ列に、電子バリュー提供者によるデジタル署名(1416)を施したものである。

【0151】

そして、電子バリュー発行システム106は、モバイルECサーバ104へ、その電子バリューに対応する電子バリューの発行処理と電子バリュー代金の決済処理とを依頼するメッセージ、電子バリュー発行依頼1518を送信する。電子バリュー発行依頼1518には、申込まれた電子バリューの電子バリューデータが含まれる。

【0152】

電子バリュー発行依頼1518を受信したモバイルECサーバ104の電子バリュー発行処理部805は、電子バリュー発行依頼1518を、司令部806へ送信する。司令部806は、電子バリュー発行依頼1518に基づいて、電子バリューの代金の決済処理と電子バリューの発行処理とを行なう。

【0153】

まず、司令部806は、電子バリュー発行システム106から受信した電子バリュー発行依頼1518に含まれる決済処理の内容を示すメッセージ、決済要求1519を、決済処理部に送信する。決済要求1519を受信した決済処理部は、決済要求1519に基づいて電子バリュー代金の決済処理を要求するメッセージ、代金決済要求1520を

生成して、決済処理システム106へ送信する。

【0154】

決済処理システム106は、受信した決済要求1519に基づいて、決済処理を行なう。そして、決済処理結果を含む決済完了を通知するメッセージ、決済処理結果1521を生成し、モバイルECサーバ104に送信する。

【0155】

決済処理結果1521を受信したモバイルECサーバ104の決済処理部は、決済処理結果1521を司令部806に送る。司令部806は、決済処理結果1521の中の電子バリュー発行者に関する情報を電子バリュー発行システムに通知することを要求するメッセージ、完了通知1522を、電子バリュー発行処理部805に送信し、電子バリュー発行処理部805が、電子バリュー発行者に対する決済完了のメッセージ、決済完了通知1523を生成し、電子バリュー発行システムに送信する。決済完了通知1523には、決済処理結果が含まれる。電子バリュー発行処理部805から、決済完了通知1523を受信した電子バリュー発行システム106は、決済処理を受信したことを通知するメッセージ、決済確認通知1524を生成して、モバイルECサーバ104へ送信する。

【0156】

司令部806は、電子バリュー発行システム106への決済完了通知1522を行った後、ユーザ1500に発行する電子バリューと領収書を生成し、電子バリューの送信を要求するメッセージ、送信要求1525を、ユーザ処理部802に送信する。送信要求1525には、生成した電子バリューと領収書が含まれる。送信要求1525を受信したユーザ処理部802は、電子バリューを送信するメッセージ、電子バリュー送信1526を、デジタル無線電話通信で、モバイルユーザ端末100へ送信する。

【0157】

電子バリュー送信1526は、図19(c)に示すように、電子バリュー送信だということを示すメッセージID1707と、モバイルECサーバ104の秘密鍵で署名した(1710)電子バリュー178と、モバイルECサーバ104の秘密鍵で署名した(1710)領収書1709をユーザ1500の公開鍵で封書化した(1711)ものを含む。

【0158】

また、司令部806による電子バリューの生成は、次の手順で行なわれる。

まず、司令部806は、電子バリュー情報の中の使用条件情報をもとに、電子バリューステータス1404と、電子バリュープロパティ1405を生成する。例えば、バス乗車回数券の場合には、電子バリュープロパティ1405として、回数券の初期枚数と使用済枚数（発行時はゼロに設定）が設定される。そして、司令部806は、新たに、電子バリュー署名秘密鍵1406と電子バリュー署名公開鍵の鍵対を生成し、さらに、電子バリュー管理情報1306に登録されている電子バリュー認証秘密鍵1406と、トランザクション端末認証公開鍵1408とを用いて、電子バリューの電子バリュープログラム1401を生成する。

【0159】

さらに、司令部806は、生成した電子バリュー署名公開鍵をもとに、電子バリューの電子バリュー証明書1403を生成し、電子バリューの発行を依頼するメッセージをもとに電子バリューの提示電子バリュー1402を生成して、電子バリュー1400を生成する。

【0160】

一方、電子バリュー送信1526を受信したモバイルユーザ端末100は、電子バリュー1708と領収書1709を、ユーザ1500の秘密鍵で復号化し、それぞれ、デジタル署名をチェックし、有効だった場合、電子バリュー1708を電子バリューリスト710に登録し、領収書1709を使用履歴リスト711に登録する。

【0161】

また、デジタル署名の有効性が確認された場合、モバイルユーザ端末100は、電子バリューを受信したことを示すメッセージ、確認通知1527を、モバイルECサーバ104に送信し、図18(d)に示すように、モバイルユーザ端末100のLCDに電子バリューを表示する（電子バリューの表示1528）。確認通知1527は、図19(d)に示すように、電子バリュー送信1526に対する応答メッセージだということを示すメッセージID1712と、領収書1709をハッシュ演算してユーザの秘密鍵で暗号化したデータ(1714)を含む。

【0162】

確認通知1527を受信したモバイルECサーバ104のユーザ処理部802は、受信し

た領収書と送信した領収書を比較し、一致した場合、電子バリューの送信処理が完了したことを示すメッセージ、送信完了1529を司令部806に送り、送信完了1529を受信した司令部806は、購入処理の完了を示すメッセージ、購入完了1530をWWWサーバ803に送信する。購入完了1530を受信したWWWサーバ803は、購入完了1530を、ホーム端末103に送信する。購入完了1530を受信したホーム端末103は、図18(e)に示すように、受信した購入完了1530に基づいて、ユーザ1500に、ユーザ1500が要求したオーダが完了した旨を表示する（完了表示1531）。

【0163】

これにより、ホーム端末を用いて電子バリューを申し込み、購入した電子バリューをモバイルユーザ端末にダウンロードして、使用することができ、受け取りに行く手間が省け、利便性が向上する。

また、モバイルユーザ端末にID送信機能を設けることで、入力の手間が軽減される。

また、前述の実施方法では、電子バリューは、発行されるとすぐに、モバイルECサーバ104からモバイルユーザ端末100へ送信されるが、発行した電子バリューはモバイルECサーバ104のユーザ処理部802に格納され、発行処理が終了した旨をユーザに通知し、ユーザが必要なときにモバイルECサーバ104にアクセスし、購入した電子バリューをダウンロードする場合もある。

【0164】

図16、17を用いて、ユーザが必要なときにモバイルECサーバ104にアクセスし、購入した電子バリューをダウンロードする場合を説明する。図16は、電子バリュー購入時に、電子バリューのダウンロードを別途行う場合の処理のフロー、図27(c)は、電子バリューのダウンロード処理のフローを示している。

【0165】

図27(b)に示すように、引換書送信1532までは、図15と同様である。引換書送信1532には、これが引換書送信だということを示すメッセージIDと、引換書が含まれている。この引換書は、領収書に含まれるデータに加えて、電子バリューは未送信である旨を示す情報が含まれている。引換書送信1532を受信した

モバイルユーザ端末は、引換書の電子署名を検証し、有効性だった場合、ユーザ処理部に、引換書受信要求に応答するメッセージ、引換書確認通知1533を送信し、引換書をモバイルユーザ端末に表示する(引換書表示1534)。引換書確認通知1533には、それが引換書確認通知であることを示すメッセージIDと、引換書をハッシュ演算して暗号化したデータが含まれる。これ以後の処理は、図15と同様に行われる。

【0166】

電子バリューをダウンロードするときには、図17に示すように、ユーザーが、モバイルユーザ端末100のLCDに受信した引換書を表示させ、実行ボタンを押す(ダウンロード要求操作1535)と、モバイルユーザ端末100は、モバイルECサーバ104に、購入済みの電子バリューのダウンロードを要求するメッセージ、ダウンロード要求1536を送信する。ダウンロード要求1536には、図19(e)に示すように、購入済の電子バリューのダウンロード要求であることを示すメッセージID1715と、電子バリュー未送信である旨を示す情報が含まれている領収書1716をハッシュ演算してユーザの秘密鍵で暗号化した(1717)データが含まれる。

【0167】

ダウンロード要求1536を受信したモバイルECサーバ104は、領収書の有効性を確認し、有効だった場合、電子バリューを送信する。送信の手順は、図15に示す、電子バリュー送信1526、確認通知1527、電子バリュー表示1528と同様である。

これにより、ユーザは、前もって購入した電子バリューを、使用直前にダウンロードすることができ、モバイルユーザ端末100のメモリ節約になる。

【0168】

さらに、たとえば、コンサートチケット等といった、有効期間が限定されている電子バリューについては、設定により、有効期限直前に、モバイルECサーバから電子バリューを送信する方法もある。この場合、モバイルECサーバは、設定された日時に、モバイルユーザ端末にデジタル電話通信によって接続し、ユーザが前もって購入しておいた電子バリューを送信する。この場合の電子バリュー

送信の手順は、図 15 に示す、電子バリュー送信 1526、確認通知 1527、電子バリュー表示 1528 と同様である。

これにより、前もって購入した電子バリューが、使用直前に、モバイル EC サーバから送信されることで、モバイルユーザ端末のメモリ節約になるばかりでなく、ユーザの手間も軽減される。

【0169】

次に、電子バリューの使用の処理について説明する。

まず、図 20、図 21 を用いて、モバイルユーザ端末に格納されている電子バリューの内、電子チケットをゲート端末に対して使用する処理について説明する。

【0170】

図 20 は、電子バリュー使用の処理における機器間のメッセージ交換の手順を示し、図 21 は、電子バリュー使用の処理において、機器間で交換するメッセージの内容を示し、図 4 は、ゲート端末の使用結果表示画面、図 6 (a) は、使用された電子バリューの表示画面を示している。また、図 21 で、二重線で囲まれた部分は、デジタル署名が施されている部分を示し、太線で囲まれた部分は封書化されている部分を示す。

ゲート端末 101 には、改札するチケットがあらかじめ設定されているものとする。

【0171】

まず、ユーザ 1500 は、モバイルユーザ端末 100 を電子バリューモードにし、ファンクションスイッチ（“F1”，“F2”）で、使用する電子チケットを表示させる。そして、赤外線通信ポートをゲート端末 101 の赤外線通信モジュールに向けて実行スイッチを押す（提示操作）。すると、モバイルユーザ端末 100 は、電子バリューの内容をゲート端末 101 に提示するメッセージ、プレゼンテーション 1801 を、赤外線通信で、ゲート端末 101 に送信する。

【0172】

図 21 (a) に示すように、プレゼンテーション 1801 は、メッセージがプレゼンテーション 1801 であることと、そのデータ構造を示すヘッダ情報、プレゼンテ

ーションヘッダ1900と、電子バリューの使用を要求していることを示すサービスコード1901と、この電子バリュー使用の処理をユニークに示す番号として任意に生成した要求番号1902と、使用する電子バリューの提示電子バリュー1903と、電子バリュー証明書1904と、使用する電子バリューのその時のステイタスを示す電子バリューステイタス1905と電子バリュープロパティ1906と、電子バリュー I D 1907と、このプレゼンテーション1801を発行した日時を示す発行日時1908と、生成した任意のテストパターン、トランザクション端末テストパターン1909とから成るデータであり、電子バリューステイタス1905と、電子バリュープロパティ1906と、電子バリュー I D 1907と、発行日時1908とには、電子バリュー1400の電子バリュー署名秘密鍵1410によるデジタル署名（電子バリュー署名秘密鍵で署名1911）が施され、トランザクション端末テストパターン1909は、トランザクション端末認証公開鍵1408によって暗号化されている（トランザクション端末認証公開鍵で暗号化1910）。

【 0 1 7 3 】

提示電子バリュー1903と、電子バリュー証明書1904と、電子バリューステイタス1905と、電子バリュープロパティ1906と、電子バリュー I D 1907と、発行日時1908とが、ゲート端末101（またはコンテンツサーバ102）に対して、電子バリューの内容を示す部分であり、トランザクション端末テストパターン1909は、ゲート端末101（またはコンテンツサーバ102）を認証するためのテストパターンである。

【 0 1 7 4 】

プレゼンテーション1801を受信したゲート端末101（またはコンテンツサーバ102）は、まず、プレゼンテーション1801の内容の有効性を検証し、電子バリューに内容の変更を命令するメッセージ、インストラクション1802を生成し、モバイルユーザ端末100へ送信する。

【 0 1 7 5 】

プレゼンテーション1801の有効性の検証では、ゲート端末101（またはコンテンツサーバ102）は、まず、提示電子バリューと電子バリュー証明書の有効性を検証し、次に電子バリュー証明書の電子バリュー署名公開鍵を用いて、電子バリ

ユーステイタス1905と電子バリュープロパティ1906と電子バリューID1907と発行日時1908に施された電子バリューのデジタル署名を検証し、電子バリュープロパティ1906から、使用される電子バリューとして、有効な状態であるかを検証する。

【0176】

また、インストラクション1802の生成では、ゲート端末101（またはコンテンツサーバ102）は、トランザクション端末認証秘密鍵で、トランザクション端末テストパターン1909の暗号を復号化し、任意に生成したテストパターン、電子バリューテストパターン1822を、電子バリュー認証公開鍵で暗号化する（電子バリュー認証公開鍵で暗号化1923）。

【0177】

図21（b）に示すように、インストラクション1802は、メッセージがインストラクション1802であることと、そのデータ構造を示すヘッダ情報、インストラクションヘッダ1912と、インストラクション番号1913と、応答メッセージ1914と、要求番号1915と、電子バリューID1916と、インストラクションコード1917と、暗号を復号化したトランザクション端末テストパターン1918と、任意に生成したテストパターン、電子バリューテストパターン1922と、ゲート端末ID/コンテンツサーバID1919と、マーチャントID1920と、このインストラクション1802を発行した日時を示す発行日時1921とから成るデータにマーチャントのデジタル署名を行い（マーチャント秘密鍵で署名1924）、さらにマーチャント証明書を付加したものであり、電子バリューテストパターンは、電子バリュー認証公開鍵によって暗号化されている（電子バリュー認証公開鍵で暗号化1923）。

【0178】

インストラクション番号1913は、ゲート端末101（またはコンテンツサーバ102）が、この電子バリューの使用の処理をユニークに示す番号として任意に生成した番号であり、プレゼンテーション1801の検証の結果、電子バリュー使用の処理ができない場合（例えば、そのゲート端末101（またはコンテンツサーバ102）では、使用できない電子バリューであった場合）、ゼロが設定され、電子バリュー使用の処理ができる場合には、ゼロ以外の値が設定される。

【 0 1 7 9 】

応答メッセージ1914は、マーチャントからユーザ1500へのメッセージを示すテキスト情報である。ゲート端末101（またはコンテンツサーバ102）が、提示された電子バリューを使用できない場合（インストラクション番号の値がゼロの場合）、応答メッセージ1914には、電子バリューを使用できない旨を示すメッセージ設定される。応答メッセージ1914は、オプションで設定される情報であり、設定されない場合もある。

【 0 1 8 0 】

インストラクションコード1917は、電子バリューに対するコマンドコードであり、電子バリューの電子バリューステータス1905と、電子バリュープロパティ1906を、どのように変更するかを示すコード情報である。

【 0 1 8 1 】

インストラクション1802を受信したモバイルユーザ端末100は、まず、インストラクション1802の内容の有効性を検証し、有効だった場合に、インストラクションコード1805にしたがって、電子バリューの電子バリューステータス1404と電子バリュープロパティ1405を変更し、さらに、電子バリュー認証秘密鍵1407で、電子バリューテストパターン1922の暗号を復号化して、電子バリューの内容の変更を証明するメッセージ、トランザクション1803を生成し、ゲート端末101（またはコンテンツサーバ102）へ送信する。インストラクション1802の内容の有効性を検証では、まず、トランザクション端末テストパターン1909と、インストラクション1802に含まれるトランザクション端末テストパターン1918とを照合して、ゲート端末101（またはコンテンツサーバ102）の認証を行ない、次に、マーチャント証明書の有効性を検証し、さらに、マーチャントによるデジタル署名をチェックする。また、電子バリューの電子バリューステータス1404と電子バリュープロパティ1405の変更では、例えば、電子バリューが一回のみ有効なチケットの場合、電子バリューステータスを使用不可に変更する。また、電子バリューが回数券で、電子バリュープロパティに、初期値が5、使用回数が3に設定されていた場合、電子バリューステータスは有効のまま変更せず、使用回数を4にインクリメントする。

【0182】

図21に示すように、トランザクション1803は、メッセージがトランザクション1803であることと、そのデータ構造を示すヘッダ情報、トランザクションヘッダ1925と、電子バリューの使用の処理の順番を示すトランザクション番号1926と、暗号を復号化した電子バリューテストパターン1927と、変更後の電子バリューステータス1928と電子バリュープロパティ1929と、電子バリュープロパティ1929の変更前後の差分の値を示す電子バリュー変化値1948と、ゲート端末ID/コンテンツサーバID1930と、マーチャントID1931と、要求番号1932と、インストラクション番号1933と、電子バリューコード1934と、電子バリューID1935と、このトランザクション1803を発行した日時を示す発行日時1936とから成るデータについて、電子バリュー署名秘密鍵によるデジタル署名と、ユーザ1500のデジタル署名を行なったものである（チケット署名秘密鍵で署名・ユーザ秘密鍵で署名1937）。

【0183】

トランザクション1803を受信したゲート端末101（またはコンテンツサーバ102）は、まず、電子バリューテストパターン1922と、トランザクション1803に含まれる電子バリューテストパターン1927とを照合して、電子バリューの認証を行ない、一致した場合、さらに、トランザクション1803の内容の有効性を検証し、有効だった場合、電子バリューの使用の領収書に相当するメッセージ、レシート1804を生成して、モバイルユーザ端末100へ送信する。

【0184】

トランザクション1803の有効性の検証では、ゲート端末101（またはコンテンツサーバ102）は、電子バリューステータス1903と電子バリュープロパティ1904と電子バリュー変化値1948が、インストラクションコード1917にしたがって変更されているかを検証し、トランザクション1803の電子バリューのデジタル署名1937をチェックする。電子バリュー変化値1948は、電子バリューがチケットの場合には、通常1が設定され、電子プリペイドカードの場合には、対象トランザクション処理で使用された金額が設定されている。

【0185】

図 2 1 (d) に示すように、レシート1804は、メッセージがレシート1804であることと、そのデータ構造を示すヘッダ情報、レシートヘッダ1938と、電子バリュー使用処理の内容を示すテキスト情報、トランザクション情報1939と、要求番号1940と、電子バリュー I D 1941と、インストラクション番号1942と、トランザクション番号1943と、ゲート端末 I D / コンテンツサーバ I D 1944と、マーチャント I D 1945と、このレシート1804を発行した日時を示す発行日時1946とから成るデータについて、マーチャントのデジタル署名を行なった（マーチャント秘密鍵で署名1947）ものである。

【 0 1 8 6 】

レシート1804を受信したモバイルユーザ端末100は、レシート1804の内容の有効性を検証し、有効だった場合、レシート1804からアクノーリッジ1805を生成して、ゲート端末101またコンテンツサーバ102に送信し、レシート1804を、使用情報として、使用履歴リスト711に登録し、図 6 (a) に示すように、L C D に使用した電子バリューを表示する（使用されたチケットの表示1806）。

レシート1804の有効性の検証では、モバイルユーザ端末100は、レシート1804のマーチャントのデジタル署名1937をチェックする。

【 0 1 8 7 】

アクノーリッジ1805は、レシート1804をハッシュ演算してダイジェストを生成し、それを電子バリューの秘密鍵で暗号化したものである。

【 0 1 8 8 】

アクノーリッジ1805を受信したゲート端末101（またはコンテンツサーバ102）は、受信したアクノーリッジ1805を電子バリューの公開鍵で復号化してダイジェストを生成し、送信したレシート1804をハッシュ演算して生成したダイジェストと照合して、署名の検証を行う。一致した場合、トランザクション1803を、電子バリュー使用処理の履歴情報として、トランザクション1803履歴リスト511に登録する。

【 0 1 8 9 】

さらに、ゲート端末101は、図 4 に示すように、タッチパネル L C D 401に、使用処理結果を表示する。マーチャントは、タッチパネル L C D 401に表示された

使用処理結果に基づいて、ユーザ1500の入場を許可する表示を行う（使用結果表示・入場許可1807）。また、ゲート端末101に、ゲート開閉装置が接続されている場合には、自動的にゲートが開かれる（使用結果表示・入場許可1807）。

【0 1 9 0】

以上のように、ゲート端末101（またはコンテンツサーバ102）は、モバイルユーザ端末100と電子バリューの正当性を確認し、モバイルユーザ端末100は、ゲート端末101（またはコンテンツサーバ102）の正当性を確認し、また、実行された決済の正当性を確認でき、より安全な決済が実現できる。

【0 1 9 1】

次に、図 2 2 および図 2 3 を用いて、コンテンツサーバ102からホーム端末103に提供されるサービスの代金を、モバイルユーザ端末に格納された電子バリューを使用して支払う処理について説明する。この場合、モバイルユーザ端末に格納された電子バリューの内、電子プリペイドカードを使用する。

図 2 2 は、電子バリュー使用の処理における機器間のメッセージ交換の手順を示し、図 2 3 は、電子バリュー使用時の画面表示の例を示している。

まず、ユーザ1500は、ホーム端末103からデジタル公衆網108を介してコンテンツサーバ102にアクセスし、提供を受けたいサービスを選択する（サービス要求操作2000）。

【0 1 9 2】

ホーム端末103は、ユーザ1500のサービス要求をコンテンツサーバ102に提示するメッセージ、サービス要求情報2001をコンテンツサーバ102に送信する。

【0 1 9 3】

サービス要求情報2101を受信したコンテンツサーバ102は、モバイルユーザ端末100に電子バリューの提示を要求するメッセージ、電子バリュー提示要求情報2002を、ホーム端末103に送信する。

この電子バリュー提示要求情報2002には、モバイルユーザ端末100を認証するための番号、要求番号と、コンテンツサーバの電話番号が含まれている。

電子バリュー提示要求情報2002を受信したホーム端末103は、図 2 3 (a) に示すように、ユーザに電子バリューの使用を促す旨を表示する（提示要求表示20

03)。

【0 1 9 4】

ユーザ1500は、モバイルユーザ端末100を電子バリュモードにして、ファンクションスイッチ（“F1”，“F2”）で、LCDに、使用する電子バリュを表示させる。図23（b）に示すように、“電話番号”を入力するエントリと“要求番号”を入力するエントリがLCDに表示される。ユーザが、それぞれのエントリに、ホーム端末103に表示された電話番号と要求番号をキー入力し、実行スイッチを押す（提示操作2004）と、モバイルユーザ端末100は、電子バリュをコンテンツサーバ102に提示するメッセージ、プレゼンテーション1801を生成する。さらに、モバイルユーザ端末100は、入力された電話番号を参照し、コンテンツサーバ102にデジタル電話通信接続し、生成したプレゼンテーション1801をコンテンツサーバ102に送信する。このとき、プレゼンテーション1801の要求番号1902には、ユーザが入力した要求番号が設定される。

【0 1 9 5】

プレゼンテーション1801を受信したコンテンツサーバ102は、要求番号と電子バリュの種類を検証し、要求番号が一致し、電子バリュの種類も有効だった場合、インストラクション1802を、モバイルユーザ端末100へ送信する。

【0 1 9 6】

インストラクション1802を受信したモバイルユーザ端末100は、インストラクション1802に基づいて電子バリュを変更し、トランザクション1803を、コンテンツサーバ102に送信する。

トランザクション1803を受信したコンテンツサーバ102は、トランザクション1803の内容を検証し、レシート1804を、モバイルユーザ端末100へ送信する。

レシート1804を受信したモバイルユーザ端末100は、レシート1804の内容を検証し、アクノーリッジ1805をコンテンツサーバ102コンテンツサーバ102に送信する。そして、モバイルユーザ端末100は、図23（c）に示すように、LCDに使用後の電子バリュを表示する（使用された電子バリュの表示2005）。

【0 1 9 7】

アクノーリッジ1805を受信したコンテンツサーバ102は、受信したアクノーリ

ッジ1805の検証を行ない、アクノーリッジ1805が有効であった場合に、ホーム端末103に対して、サービス情報を送信する（コンテンツ情報2006）。サービス情報を受信したホーム端末103は、受信したサービス情報をテレビモニタに表示する（サービス表示2007）。

【0198】

以上において、モバイルユーザ端末100とコンテンツサーバ102の間で交換されるプレゼンテーション、インストラクション、トランザクション、レシート、アクノーリッジの各メッセージの内容は、それぞれ、モバイルユーザ端末100とゲート端末101の間で交換されるプレゼンテーション、インストラクション、トランザクション、レシート、アクノーリッジの各メッセージの内容と同じである。

【0199】

なお、コンテンツサーバ102からホーム端末103に提供されるサービスの代金の支払に、電子バリュー情報1412としてコンテンツサーバ102の電話番号が埋め込まれた電子バリュー（電子プリペイドカード）を使用しても良い。この場合、モバイルユーザ端末は、電子バリュー情報1412の電話番号を参照して、コンテンツサーバにデジタル電話通信接続する。したがって、この場合、ユーザは、電子バリューを使用する際にコンテンツサーバの電話番号を入力する必要がない。

また、このコンテンツサーバからは、大きくわけて、物品、電子チケット、デジタル情報、放送視聴権の4種類の購入が可能である。

【0200】

まず、物品の場合、購入申込みをした物品は配送され、サービス表示2007では、テレビモニタに、配送予定日などが表示される。

また、電子チケットの場合、コンテンツサーバから依頼を受けたモバイルECシステムから、モバイルユーザ端末に電子チケットが送信され、サービス表示2007では、テレビモニタに、モバイルユーザ端末に電子チケットを送信した処理結果等が表示される。

また、デジタル情報の場合、コンテンツ情報2006に購入したデジタルデータが含まれ、サービス表示2007では、テレビモニタに、購入した情報が表示される。

【0201】

また、放送視聴権の場合、コンテンツ情報2006には購入したチャンネルのチャンネル鍵が含まれ、コンテンツ情報2006を受信したホーム端末は、チャンネル鍵をEEPROM303に格納する。これにより、ホーム端末103は、放送視聴権を購入したチャンネルのスクランブル鍵の復号化をして、そのチャンネルの視聴が可能な状態となり、サービス表示2007では、テレビモニタ上にそのチャンネルの番組を表示する。ここで、EEPROMの代わりに、ICカードが用いられている場合には、チャンネル鍵はICカードに格納され、スクランブル鍵の復号化もICカードによって行われる。

【0202】

例えば、図23(a)に示すように、デジタル画像と放送視聴権を購入した場合には、購入したデジタル画像と放送を視聴するためのチャンネル鍵がコンテンツサーバ102からホーム端末103に送信される（コンテンツ情報2006）。ホーム端末103は、受信したデジタル画像を、テレビモニタに表示し（サービス表示2007）、受信したチャンネル鍵をEEPROM303に格納する。そして、ユーザが、テレビモニタを切り替え、購入したチャンネルを表示させると、スクランブルが復号化された放送が視聴できる（サービス表示2007）。

【0203】

以上のように、物品と、電子チケットと、ネットワーク情報サービス（デジタル情報）と、放送サービス（放送視聴権）が融合したオンライン売買が可能となる。例えば、教育関係では、テキスト（物品）と、対面レッスンのチケット（電子チケット）と、インターネットを使った添削サービス（ネットワーク情報サービス）と、講義（放送サービス）とを組み合わせたサービス、また、音楽関係では、CD（物品）と、コンサートのチケット（電子チケット）と、インターネットライブ（ネットワーク情報サービス）を組み合わせたサービスの提供が可能となる。このように、今までは、別々に売買されていたものを、まとめてオンラインで提供することにより、消費者の利便性が向上し、また、提供側にとっても商品の付加価値を高め、販売促進につながる。

（実施の形態2）

本発明の第2の実施の形態は、ホーム端末を介し、モバイルユーザ端末に格納された電子バリューを、コンテンツサーバとの取引に使用するように構成したものである。

以下、本発明の第2の実施の形態について、図24および図25を用いて説明する。本実施の形態は、システム構成および電子バリュー購入の手順は、実施の形態1と同様である。したがって、実施の形態1と異なる電子バリューの使用について説明する。

【0204】

図24は、インターネット上のサービス利用などにおいて、ホーム端末103を介してコンテンツサーバ102に電子バリューを送信する場合の電子バリュー使用の処理の手順を示し、図25は、電子バリュー使用時の画面表示例を示している。

【0205】

まず、ユーザ1500は、ホーム端末103からデジタル公衆網108を介してコンテンツサーバ102にアクセスし、利用したいサービスを選択する（サービス要求操作2000）。

【0206】

ホーム端末103は、ユーザ1500のサービス要求をコンテンツサーバ102に提示するメッセージ、サービス要求情報2001を、コンテンツサーバ102に送信する。

【0207】

サービス要求情報2001を受信したコンテンツサーバ102は、モバイルユーザ端末100に電子バリューの提示を要求する電子バリュー提示要求情報2002を、ホーム端末103に送信する。

【0208】

電子バリュー提示要求情報2002を受信したホーム端末103は、電子バリュー対応のプラグインアプリケーションを起動し（プラグインアプリケーション起動2200）、次に、図25（a）に示すように、テレビモニタに電子バリューの使用を促す旨を表示し（提示要求表示1801）、電子バリューの使用を要求するメッセージ、電子バリュー提示要求2203を赤外線通信モジュール201から送信し続ける。

【0209】

ホーム端末103の表示を見たユーザ1500は、図25(b)に示すように、モバイルユーザ端末100を電子バリューモードにし、ファンクションスイッチ(“F1”, “F2”)でLCDに使用する電子バリューを表示して、実行スイッチを押す(提示操作2202)。すると、モバイルユーザ端末100は、赤外線通信の受信モードとなり、ホーム端末103から送信されている電子バリュー提示要求2203を受信する。電子バリュー提示要求2203を受信したモバイルユーザ端末100は、電子バリューの内容をコンテンツサーバ102に提示するメッセージ、プレゼンテーション1801を、赤外線通信で、ホーム端末103に送信する。さらに、プレゼンテーション1801を受信したホーム端末103は、デジタル電話通信によってコンテンツサーバ102にプレゼンテーション1801を送信する。

【0210】

プレゼンテーション1801を受信したコンテンツサーバ102は、電子バリューの種類を検証し、インストラクション1802を、デジタル電話通信によってホーム端末103に送信する。さらに、インストラクション1802を受信したホーム端末103は、インストラクション1802を赤外線通信でモバイルユーザ端末100へ送信する。

【0211】

インストラクション1802を受信したモバイルユーザ端末100は、インストラクション1802に基づいて電子バリューを変更し、トランザクション1803を、赤外線通信で、ホーム端末103に送信する。さらに、トランザクション1803を受信したホーム端末103は、トランザクション1803を、デジタル電話通信によってコンテンツサーバ102に送信する。

【0212】

トランザクション1803を受信したコンテンツサーバ102は、トランザクション1803の内容を検証し、レシート1804を、デジタル電話通信によってホーム端末103に送信する。さらに、レシート1804を受信したホーム端末103は、レシート1804を赤外線通信でモバイルユーザ端末100へ送信する。

【0213】

レシート1804を受信したモバイルユーザ端末100は、レシート1804の内容を検

証し、アクノーリッジ1805を、赤外線通信で、ホーム端末103に送信するさらに、アクノーリッジ1805を受信したホーム端末103は、デジタル電話通信によってアクノーリッジ1805をコンテンツサーバ102に送信し、プラグインアプリケーションを終了する（プラグインアプリケーション終了2207）。そして、モバイルユーザ端末100は、図23（c）に示すように、LCDに使用後の電子バリューを表示する（使用された電子バリューの表示2204）。

【0214】

アクノーリッジ1805を受信したコンテンツサーバ102は、受信したアクノーリッジ1805の検証を行ない、アクノーリッジ1805が有効であった場合に、ホーム端末103にサービス情報（インターネットライブデータ等）を送信する（コンテンツ情報2205）。サービス情報を受信したホーム端末103は受信したサービス情報をテレビモニタに表示する（インターネットライブ等）（サービス表示2206）。

【0215】

ホーム端末は、アクノーリッジ1805を送信するとプラグインアプリケーションを終了する（プラグインアプリケーション終了2207）。

また、本実施の形態におけるプレゼンテーション1801、インストラクション1802、トランザクション1803、レシート1804、アクノーリッジ1805のメッセージの内容は実施の形態1と同様である。

【0216】

以上のようにモバイルユーザ端末100は、新たにコンテンツサーバ102と直接通信接続することなく、近距離にあるホーム端末と赤外線通信を行うことで、サービスの提供が受けられ、通信コストが軽減される。また、使用時に、ユーザの入力の手間を軽減される。

（実施の形態3）

本発明の第3の実施の形態は、モバイルユーザ端末に格納された電子バリューを、視聴した有料放送の代金の支払に使用するように構成したものである。以下、本発明の第3の実施の形態について、図26および図27を用いて説明する。本実施の形態は、システム構成および電子バリュー購入の手順は、実施の形

態1と同様である。したがって、実施の形態1と異なる電子バリューの使用について説明する。

【0217】

図26は、ホーム端末103に格納された有料放送の課金情報に基づいて、コンテンツサーバ102に対して電子バリューを使用する場合の処理の手順を示し、図27は、電子バリュー使用時の画面表示例を示している。

【0218】

本実施の形態では、ホーム端末のROM301には、有料放送の課金と精算を行うアプリケーションプログラム、課金プログラムが格納され、また、コンテンツサーバ102からは、放送局に代わって、有料放送の視聴料を精算するサービスが提供される。有料放送のチャンネル鍵は、テレビ信号とともに送信され、ホーム端末のEEPROM303またはICカードに格納される。ユーザーが、リモコンを用いて、有料放送を視聴する操作を行うと、ホーム端末は、チャンネル鍵でスクランブル鍵を復号化し、チューナで番組のスクランブルをデコードして、テレビモニタに表示する。このチャンネル鍵でスクランブル鍵を復号化したときに、課金プログラムによって課金処理が発生し、課金情報が、EEPROM303またはICカードに格納される。ホーム端末は、この課金情報の合計が一定額以上になると、課金プログラムにより、有料放送が視聴できなくなる。この課金情報の精算に対して、ユーザは、モバイルユーザ端末に格納された電子バリューを使用する。

【0219】

まず、ユーザ1500は、リモコン204で操作して、ホーム端末103に、電子バリューを適用したい課金情報を表示する（精算要求操作2400）。

【0220】

精算要求操作2400を受けたホーム端末103は、電子バリュー対応のアプリケーションを起動し（アプリケーション起動2401）、図27(a)に示すように、テレビモニタに電子バリューの使用を促す旨を表示し（提示要求表示2402）、コンテンツサーバ102にプレゼンテーション1801を送信することを要求するメッセージ、電子バリュー提示要求2404を赤外線通信モジュール201から送信し続ける。

【0221】

電子バリュー提示要求2404には、プレゼンテーション1801送信を要求することを示すメッセージIDと、課金情報（視聴履歴）と、コンテンツサーバの電話情報が含まれる。

【0222】

ホーム端末103の表示を見たユーザ1500は、モバイルユーザ端末100を電子バリューモードにし、ファンクションスイッチ（“F1”, “F2”）でLCDに使用する電子バリューを表示して、実行スイッチを押す（提示操作2403）。提示操作2403を行うと、モバイルユーザ端末100は、赤外線通信の受信モードとなり、ホーム端末103から送信されている電子バリュー提示要求2404を受信する。電子バリュー提示要求2404を受信したモバイルユーザ端末100は、電子バリューの内容をコンテンツサーバ102に提示するメッセージ、プレゼンテーション1801を、電子バリュー提示要求2404に含まれる電話情報を参照して、デジタル電話通信で、コンテンツサーバ102に送信する。

【0223】

プレゼンテーション1801の内容は、実施の形態1と同様であるが、本実施の形態では、トランザクション端末認証公開鍵で暗号化した課金情報（視聴履歴）も含まれる。

プレゼンテーション1801を受信したコンテンツサーバ102は、電子バリューの種類を検証し、有効だった場合、課金情報を格納して、インストラクション1802を、モバイルユーザ端末100へ送信する。

【0224】

インストラクション1802の内容は、実施の形態1と同様である。

インストラクション1802を受信したモバイルユーザ端末100は、インストラクション1802に基づいて電子バリューを変更し、トランザクション1803を、コンテンツサーバ102に送信する。

【0225】

トランザクション1803の内容は、実施の形態1と同様である。

トランザクション1803を受信したコンテンツサーバ102は、トランザクション1

803の内容を検証し、有効だった場合、レシート1804を、モバイルユーザ端末100へ送信する。

【0226】

レシート1804の内容は、実施の形態1と同様であるが、本実施の形態では、レシート1804のトランザクション1803情報には、マーチャント鍵でデジタル署名された精算処理結果が含まれている。

【0227】

レシート1804を受信したモバイルユーザ端末100は、レシート1804の内容を検証し、アクノーリッジ1805を、コンテンツサーバ102に送信する。アクノーリッジ1805の内容は、実施の形態1と同様である。

【0228】

アクノーリッジ1805を受信したコンテンツサーバ102は、受信したアクノーリッジ1805の検証を行ない、アクノーリッジ1805が有効であった場合に、コンテンツサーバは、アクノーリッジ1805をトランザクション履歴リスト509に登録する。精算処理は、実施の形態1と同様に行われる。

【0229】

一方、モバイルユーザ端末100は、電子バリュー提示要求2404に応答するメッセージ、電子バリュー提示応答2405を、赤外線通信で、ホーム端末104に送信する。そして、モバイルユーザ端末100は、LCDに使用された電子バリューを表示する（使用された電子バリューの表示2406）。電子バリュー提示応答2405には、電子バリュー提示要求2404に対する応答であることを示すメッセージIDと、マーチャント鍵でデジタル署名された処理結果が含まれる。

【0230】

電子バリュー提示応答2405を受信したホーム端末は、受信した処理結果を検証し、有効だった場合、受信した処理結果を基に、格納されている課金情報を精算し、図27(b)に示すように、処理結果をユーザに表示する（結果表示2407）

ユーザがリモコンを操作し、課金情報画面が消されると（精算終了操作2408）、アプリケーションも終了する（アプリケーションの終了2409）。

【0231】

これにより、ユーザは、電子バリューを、ホーム端末の有料サービス受信に対する課金情報にも使用することができ、利便性が向上する。一方、テレビ放送など、データを一方向に送信するサービスを提供している事業者にとっても、サービス提供先の端末（ホーム端末）の課金情報を得るための手段を新たに設ける必要がなく、負担が軽減する。

【0232】

【発明の効果】

以上のように、本発明は第1に、

無線通信手段を有する電子財布から、前記無線通信手段を通じて、必要な対価を支払い、供給側から商品やサービスの提供または必要な許可を受けるモバイル・エレクトロニックコマース・システムにおいて、

サービス提供手段が、指示閲覧手段から受信した購入要求に基づいて、電子的な有価カードのプログラムである電子バリューを、無線通信によって電子財布にインストールようにしたものである。

サービス提供手段は電子バリューの販売サーバ、指示閲覧手段はインターネットテレビやホームパソコンなどのホーム端末、電子財布は携帯端末を想定できる。

【0233】

これにより、わざわざプリペイドカード販売店やチケット販売店に行かなくても、指示閲覧手段を用いて申込情報をサービス提供手段に送信することにより、ユーザは家庭や職場にしながら、電子プリペイドカードや電子チケットといった電子バリューを入手することができ、利便性が向上する。

また、ホーム端末を指示閲覧手段として利用することにより、電子財布よりも、大きな画面をみながら、購入する電子バリューを選択することができる。

【0234】

第2に、

サービス提供手段が、発行した電子バリューを、電子バリューごとに設定された日時に、電子財布にインストールものであり、

これにより、電子バリューが有効になる期日直前に電子バリューを自動的に送信するといったことができ、使用しない電子バリューを電子財布に格納しないことで、電子財布のメモリの使用効率が向上する。

【0235】

第3に、

サービス提供手段が、前記電子財布による対価の支払と電子バリューの未領収を証明する引換証を電子財布に発行するものであり、

この引換証により、電子バリューに対する支払を確認（ユーザは支払いと電子バリューの未領収を証明）することができ、取引の信頼性が向上する。

【0236】

第4に、

供給側が、放送の復号化処理に用いる鍵情報を指示閲覧手段に提供するものであり、

これにより、従来の有料放送システムに限らず、モバイル・エレクトロニック・システムにおいても、放送の復号化処理に用いる鍵情報の売買が可能となり、有料放送の提供方法の選択肢が増える。

【0237】

第5に、

電子財布が、無線通信で、引換証に対応する電子バリューのインストールを所定の機関に要求するものであり、

これにより、電子財布の所有者の必要なときに、電子バリューをダウンロードでき、利便性が向上する。

【0238】

第6に、

電子財布が、供給側へ対価を支払う手順の中に、次に示す手順が1つ以上含まれることを特徴とするものである。つまり、

- (1)対価の支払いを申し出るメッセージを前記供給側へ送信。
- (2)前記供給側から、対価の支払いを請求するメッセージを受信。
- (3)前記供給側への対価の支払いを証明するメッセージを前記供給側へ送信。

(4)前記供給側から、前記電子財布から電子バリューによる対価の支払を領収したことを証明するレシートメッセージを受信。

(5)前記レシートメッセージを受領したことを証明するメッセージを前記供給側へ送信。

【0239】

これにより、電子バリュー決済手段は、電子財布と電子バリューの正当性を確認し、電子財布は、電子バリュー決済手段の正当性を確認できる。また、電子バリュー決済手段と電子財布は、実行された決済の正当性を確認でき、安全性が向上する。

また、正当性の確認を目視で行う必要がないため、間違いを防ぎ、手間が軽減される。

【0240】

第7に、

電子財布が、第6の手段で示した手順を用い、指示閲覧手段を介して供給側へ対価を支払うものであり、

これにより、第6の手段を用いて対価の支払を行う電子財布は、新たに電子バリュー決済手段と直接通信回線を接続する必要なく、通信コストを削減できる。

【0241】

第8に、

電子財布が、取引の識別情報を入力する入力手段を有し、前記入力手段で入力された識別情報を供給側に送信するものであり、

これにより、取引の一意性が保証され、取引の安全性が向上する。

【0242】

第9に、

第8の手段で示した入力手段が、無線通信によって指示閲覧手段から取引の識別情報を取得する手段であるものであり、

これにより、入力の手間が省け、また、誤入力がなくなり、利便性が向上する。

【0243】

第 1 0 に、

指示閲覧手段に提供されるサービスの対価を、電子財布に格納された電子バリューにより供給側に支払うものであり、

これにより、電子財布を用いて、指示閲覧手段に提供される有料サービスの代金を支払うことができ、利便性が向上する。

【 0 2 4 4 】

第 1 1 に、

指示閲覧手段に提供されるサービスの対価を、前記指示閲覧手段に格納された履歴情報に基づいて、電子財布に格納された電子バリューにより供給側に支払うものであり、

これにより、電子財布を用いて、指示閲覧手段に提供された有料サービスの代金を支払うことができ、利便性が向上する。

【 0 2 4 5 】

第 1 2 に、

電子財布が、指示閲覧手段から、前記指示閲覧手段に格納された履歴情報を受信し、受信した履歴情報を、供給側に送信するものであり、

これにより、提供側は、指示閲覧手段に提供側に情報送信するための通信回線を持たなくても、提供されたサービスの履歴を取得することができ、効果的なサービスを提供することができる。

【 0 2 4 6 】

第 1 3 に、

電子財布が、指示閲覧手段に、提供側から受信した支払処理の結果を送信するものであり、

これにより、指示閲覧手段は、最新の支払結果に基づいて、課金プログラムを作動できる。

【 0 2 4 7 】

第 1 4 に、

指示閲覧手段が、提供されたサービスの対価の支払を、無線通信で電子財布に要求するものであり、

これにより、指示閲覧手段は、対価の支払を行う手段を持たなくても、有料サービスの提供が受けられるようになる。

【0248】

第15に、

指示閲覧手段が、通信手段を介して、供給側にサービスを要求し、供給側に対するサービスの対価の支払は、指示閲覧手段の無線通信手段を介して電子財布に要求するものであり、

これにより、提供を受ける指示閲覧手段を用いて、提供を受ける有料サービスを選択し、その支払を無線通信で接続された電子財布で行えるようになり、利便性が向上する。

【0249】

第16に、

指示閲覧手段が、通信手段を介して供給側からチャンネル鍵を取得し、チャンネル鍵を用いてスクランブル鍵にかけられた暗号を解除し、復号化されたスクランブル鍵を用いて放送のスクランブルを解除するものであり、

これにより、従来放送を介して送信されていたチャンネル鍵が、ネットワークを介して入手できるようになり、有料放送の視聴方法の選択肢が増える。

【0250】

第17に、

指示閲覧手段が、ICカード読み書き手段を有し、チャンネル鍵の格納とスクランブル鍵復号を、装着されたICカード上で行うものであり、

これにより、スクランブルの復号化に関する情報の安全性が向上する。

【0251】

第18に、

指示閲覧手段が、提供されたサービスの履歴を格納した履歴情報に基づいて、電子財布に、対価の支払を要求するものであり、

これにより、提供されたサービスの対価を、まとめて後払いすることができ、利便性が向上する。

【0252】

第 1 9 に、

指示閲覧手段が、支払処理結果を受信し、受信した処理結果に基づいて、履歴情報を変更するものであり、

これにより、第 1 8 の手段を用いて、支払を行う指示閲覧手段は、常に最新の履歴情報に基づき、課金処理を正確に行うことができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 におけるモバイル・エレクトロニックコマース・システムのブロック構成図

【図 2】

本発明の実施の形態 1 におけるホーム端末の概観図

【図 3】

本発明の実施の形態 1 におけるホーム端末のブロック構成図

【図 4】

本発明の実施の形態 1 におけるゲート端末の概観図

【図 5】

本発明の実施の形態 1 におけるコンテンツサーバに格納されるデータの模式図

【図 6】

本発明の実施の形態 1 におけるモバイルユーザ端末の概観図

【図 7】

本発明の実施の形態 1 におけるモバイルユーザ端末の RAM マップの模式図

【図 8】

本発明の実施の形態 1 におけるモバイル EC サーバのブロック構成図

【図 9】

本発明の実施の形態 1 におけるモバイル EC サーバのユーザ処理部に、一人のユーザに対して格納されるデータの模式図

【図 1 0】

本発明の実施の形態 1 におけるモバイル EC サーバのマーチャント処理部に、

一つのゲート端末、コンテンツサーバに対して格納されるデータの模式図

【図 1 1】

本発明の実施の形態 1 におけるモバイル EC サーバの決済処理部に、一つの決済処理機関に対して格納されるデータの模式図

【図 1 2】

本発明の実施の形態 1 におけるモバイル EC サーバの電子バリュー発行処理部に、一つの電子バリュー発行者に対して格納されるデータの模式図

【図 1 3】

本発明の実施の形態 1 におけるモバイル EC サーバの命令部に格納されるデータの模式図

【図 1 4】

本発明の実施の形態 1 における電子バリューのデータ構造の模式図

【図 1 5】

本発明の実施の形態 1 における電子バリュー購入に関する処理のフロー図

【図 1 6】

本発明の実施の形態 1 における電子バリュー購入（引換書）に関する処理のフロー図

【図 1 7】

本発明の実施の形態 1 における電子バリューのダウンロードに関する処理のフロー図

【図 1 8】

本発明の実施の形態 1 における電子バリュー購入の処理における画面表示例の例図

【図 1 9】

本発明の実施の形態 1 における電子バリュー購入のメッセージのデータ構造の例図

【図 2 0】

本発明の実施の形態 1 におけるユーザがゲート端末に対して電子バリューを使用する場合の処理のフロー図

【図 2 1】

本発明の実施の形態 1 における電子バリュー使用処理のメッセージのデータ構造の例図

【図 2 2】

本発明の実施の形態 1 におけるユーザがコンテンツサーバに対して直接電子バリューを使用する場合の処理のフロー図

【図 2 3】

本発明の実施の形態 1 におけるユーザがコンテンツサーバに対して直接電子バリューを使用する場合の画面表示例の図

【図 2 4】

本発明の実施の形態 2 におけるユーザがコンテンツサーバに対して間接的に電子バリューを使用する場合の処理のフロー図

【図 2 5】

本発明の実施の形態 2 における電子バリュー使用の処理における画面表示例の図

【図 2 6】

本発明の実施の形態 3 におけるユーザがホーム端末の課金情報に電子バリューを使用する場合の処理のフロー図

【図 2 7】

本発明の実施の形態 3 における電子バリュー使用の処理における画面表示例の図

【図 2 8】

従来のプリペイドカードを用いた前払い方式による決済システム、及びチケット販売システムの解説図

【符号の説明】

- 100 モバイルユーザ端末
- 101 ゲート端末
- 102 コンテンツサーバ
- 103 ホーム端末

- 104 モバイルECサーバ
- 105 決済処理システム
- 106 電子バリュー発行システム
- 107 基地局
- 108 デジタル公衆網
- 109、110、111、208 伝送路
- 112、113、114、115、116、117、118 デジタル通信回線
- 200、402、609 電源スイッチ
- 201、400、600 赤外線通信モジュール（赤外線通信ポート）
- 202 テレビモニタ
- 203、407、601 アンテナ
- 204 リモコン
- 205 映像ケーブル
- 206 音声ケーブル
- 207 アンテナケーブル
- 300 CPU
- 301 ROM
- 302 RAM
- 303 EEPROM
- 304 音声/映像処理部
- 305 チューナ
- 306 デジタル電話通信部
- 307 制御ロジック部
- 308 表示データ信号
- 309 ビデオ信号
- 400、600 赤外線通信モジュール（赤外線通信ポート）
- 401 タッチパネルLCD
- 403、608 テンキースイッチ
- 404 メニュースイッチ

- 405 ロックスイッチ
- 406 シリアルケーブル
- 602 レシーバ・スピーカ
- 603 LCD
- 604 モードスイッチ
- 605 通話スイッチ
- 606 終了スイッチ
- 607 ファンクションスイッチ
- 610 マイク
- 611 実行スイッチ
- 612 ヘッドセットジャック
- 613 ID送信ボタン
- 614 ICカードスロット
- 500、700 基本プログラム領域
- 501、701 サービスデータ領域
- 502、702 マーチャント領域
- 503、703 ワーク領域
- 504、704 テンポラリ領域
- 505、1003 マーチャント情報
- 506、1004 マーチャント公開鍵証明書
- 507、1006 マーチャント設定情報
- 508、708、906、1007 電話情報
- 509、709、907、1008 決済口座情報
- 510、1009 対象電子バリュースト
- 511、1010、1205 トランザクション履歴リスト
- 705、902 個人情報
- 706、903 ユーザ公開鍵証明書
- 707、905 ユーザ設定情報
- 710、908 電子バリュースト

711、909 使用履歴リスト
801 マーチャント処理部
802 ユーザ処理部
803 WWWサーバ
804 決済処理部
805 電子バリュー発行処理部
806 司令部
901 ユーザ名
902 ユーザ I D
904、1005 端末情報
1000 マーチャント名
1001、1931、1945 マーチャント I D
1002、1919、1930、1944 ゲート端末 I D / コンテンツサーバ I D
1100 決済処理機関名
1101 決済処理機関 I D
1102 決済処理機関情報
1103 決済処理機関公開鍵証明書
1104 決済履歴リスト
1200 電子バリュー発行者名
1201、1413 電子バリュー発行者 I D
1202 電子バリュー発行者情報
1203 電子バリュー発行者公開鍵証明書
1204 サービスコードリスト
1300 ユーザリスト
1301 マーチャントリスト
1302 決済処理機関リスト
1303 電子バリュー発行者リスト
1304 WWWサーバ情報
1305 サービス提供履歴リスト

- 1306 電子バリュー管理情報
- 1400、1708 電子バリュー
- 1401 電子バリュープログラム
- 1402、1903 提示電子バリュー
- 1403、1904 電子バリュー証明書
- 1404、1905 電子バリューステイタス
- 1405、1906 電子バリュープロパティ
- 1406 電子バリュー署名秘密鍵
- 1407 電子バリュー認証秘密鍵
- 1408 トランザクション端末認証公開鍵
- 1409 電子バリュープログラムデータ
- 1410 電子バリューコード
- 1411、1907、1916、1935、1941 電子バリュー I D
- 1412 電子バリュー情報
- 1414 サービス提供者 I D
- 1421 電子バリュー発行日時
- 1422 電子バリュー証明書ヘッダ
- 1424 電子バリュー署名公開鍵
- 1425 電子バリュー証明書 I D
- 1426 証明有効期間
- 1427 電子バリュー証明書発行日時
- 1500 ユーザ
- 1501 オーダー操作
- 1502 オーダー情報
- 1503 オファー要求
- 1504 販売オファー要求
- 1505 電子バリュー販売オファー
- 1506 オファー情報
- 1507 オファー表示

- 1508 購入操作
- 1509 購入情報
- 1510 購入認証要求
- 1511 認証情報要求
- 1512 認証要求表示
- 1513 認証確認操作
- 1514 認証情報応答
- 1515 購入認証結果
- 1516 電子バリュー購入
- 1517 電子バリュー購入申込
- 1518 電子バリュー発行依頼
- 1519 決済要求
- 1520 代金決済要求
- 1521 決済処理結果
- 1522 完了通知
- 1523 決済完了通知
- 1524 決済確認通知
- 1525 送信要求
- 1526 電子バリュー送信
- 1527 確認通知
- 1528 電子バリュー表示
- 1529 送信完了
- 1530 購入完了
- 1531 完了表示
- 1532 引換書送信
- 1533 引換書確認通知
- 1534 引換書表示
- 1535 ダウンロード要求操作
- 1536 ダウンロード要求

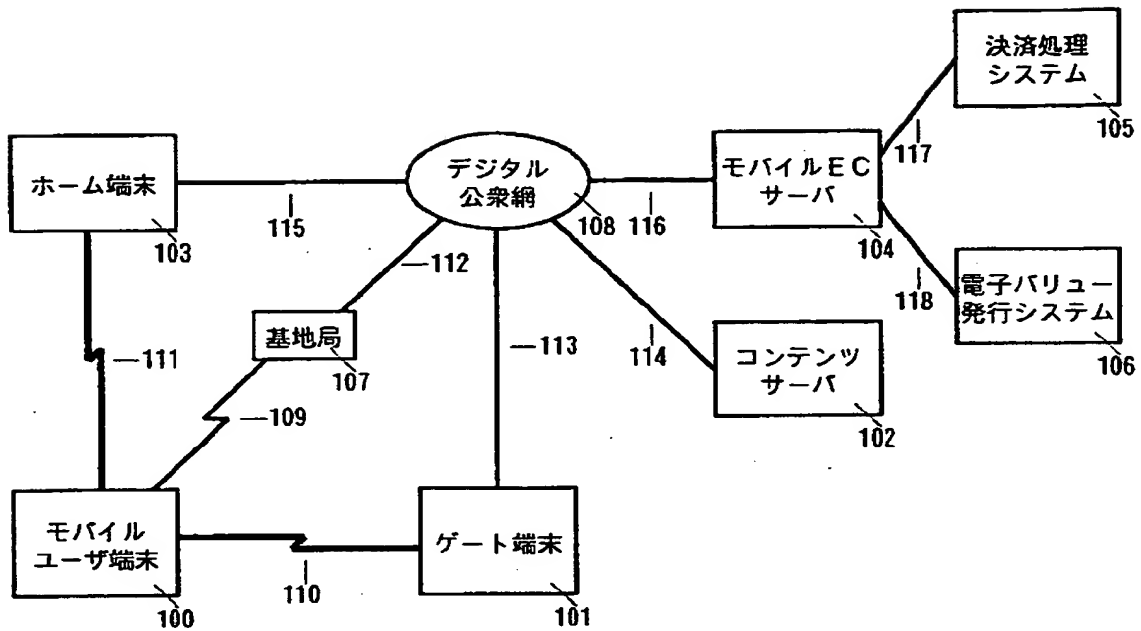
1700、1703、1707、1712、1715 メッセージID
1701、1705 乱数
1702 ユーザ公開鍵で封書化
1704、1902、1915、1932、1940 要求番号
1706 モバイルECサーバ公開鍵で封書化
1709、1713、1716 領収書
1710 モバイルECサーバ秘密鍵で署名
1711 ユーザ公開鍵で封書化
1714、1717 領収書をハッシュ演算して、電子バリュー秘密鍵で暗号化
1800 提示操作
1801 プレゼンテーション
1802 インストラクション
1803 トランザクション
1804 レシート
1805 アクノーリッジ
1806 使用されたチケットの表示
1807 使用結果表示、入場許可
1900 プレゼンテーションヘッダ
1901 サービスコード
1908、1921、1936、1946 発行日時
1909、1918 トランザクション端末テストパターン
1910 トランザクション端末認証公開鍵で暗号化
1911 チケット署名秘密鍵で署名
1912 インストラクションヘッダ
1913、1933、1942 インストラクション番号
1914 応答メッセージ
1917 インストラクションコード
1920 マーチャント証明書
1922、1927 電子バリューテストパターン

- 1923 電子バリュー認証公開鍵で暗号化
- 1924、1947 マーチャント秘密鍵で署名
- 1925 トランザクションヘッダ
- 1926、1942 トランザクション番号
- 1937 チケット署名秘密鍵で署名・ユーザ秘密鍵で署名
- 1938 レシートヘッダ
- 1939 トランザクション情報
- 1948 マーチャント証明書
- 2000、サービス要求操作
- 2001 サービス要求情報
- 2002、2404 電子バリュー提示要求情報
- 2003、2201、2402 提示要求表示
- 2004、2202、2403 提示操作
- 2005、2204、2406 使用された電子バリューの表示
- 2006、2205 コンテンツ情報
- 2007、2206 サービス表示
- 2200 プラグインアプリケーション起動
- 2203 電子バリュー提示要求
- 2207 プラグインアプリケーション終了
- 2400 精算要求操作
- 2401 アプリケーション起動
- 2405 電子バリュー提示応答
- 2407 結果表示
- 2408 精算終了操作
- 2409 アプリケーション終了
- 2600 プリペイドカード
- 2601 プリペイドカード端末
- 2602、2618 センダーシステム
- 2603 プリペイドカード販売店（自動販売機）

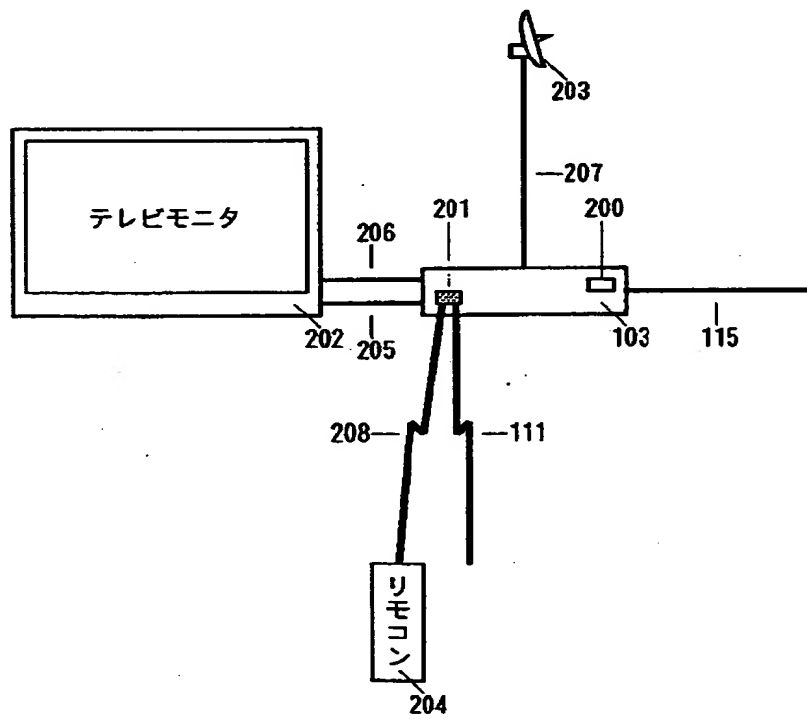
2604、2619 通信回線
2605 消費者
2606 小売販売店
2607 プリペイドカード発行者
2608 現金を払う
2609、2611、2612 プリペイドカードを渡す
2610 プリペイドカードの売上を渡す
2613 商品を渡す
2614 請求
2615 支払
2616 チケット
2617 チケット発券端末（自動発券機）
2620 チケット販売店
2621 チケット発行者
2622 受付
2623 イベント会場（イベント興行主）
2624 電話予約
2625、2626、2627 予約番号を教える
2628 チケット情報
2629 現金を渡す
2630、2632 チケットを渡す
2631 チケット売上
2633 入場許可
2634 支払

【書類名】 図面

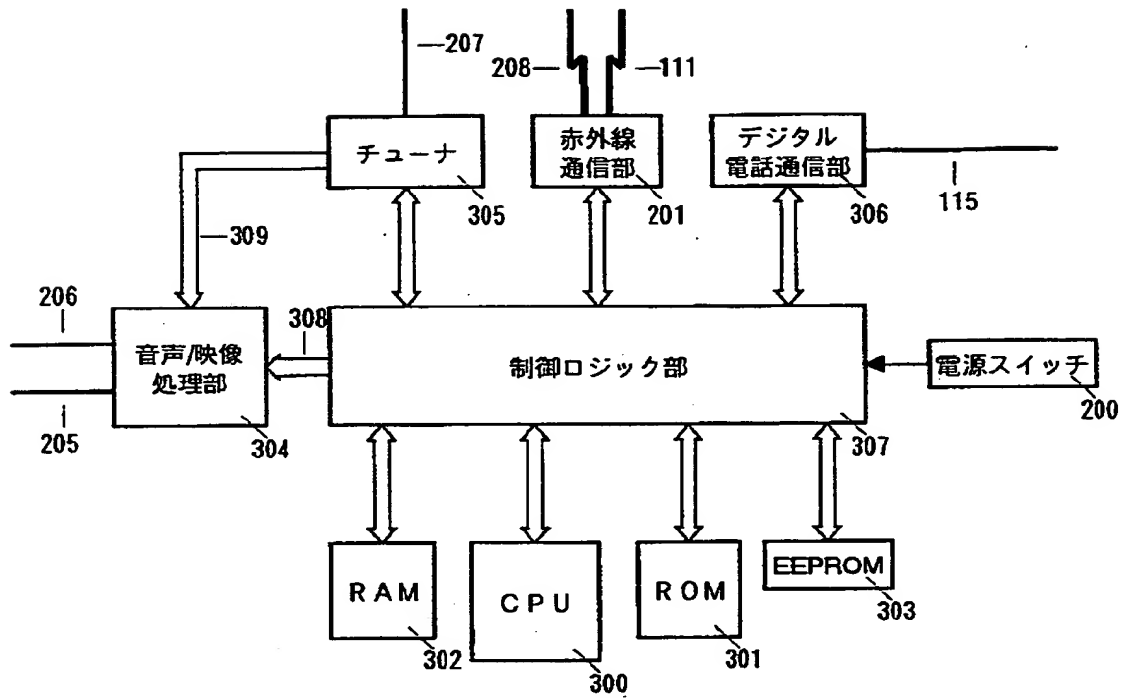
【図 1】



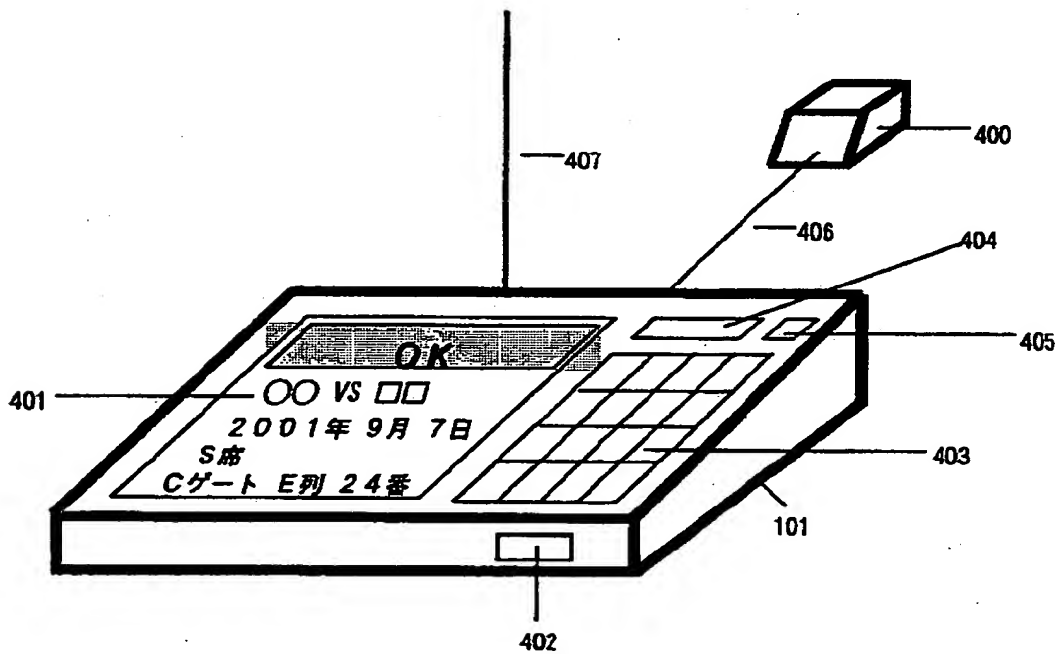
【図 2】



【図 3】



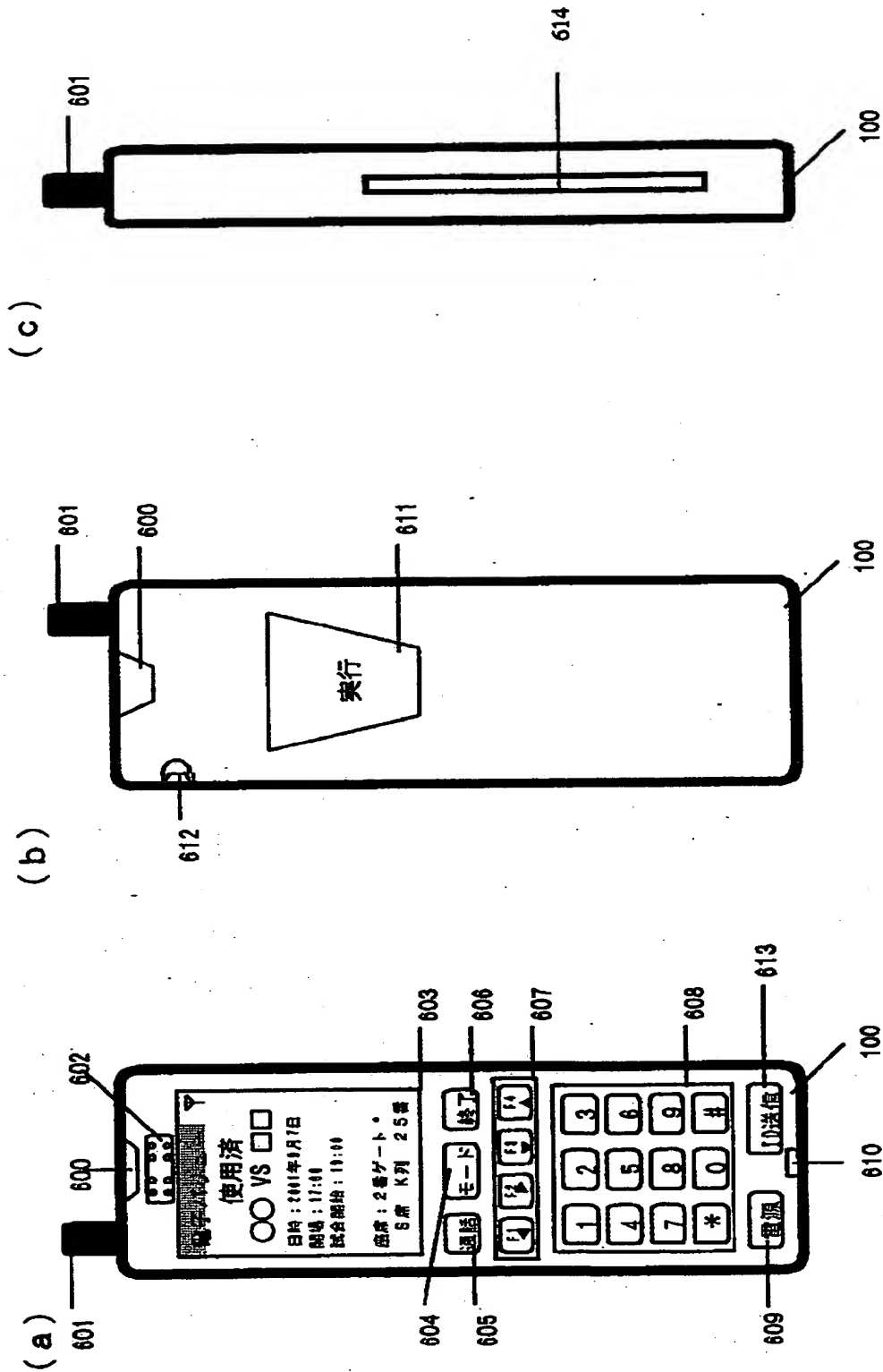
【図 4】



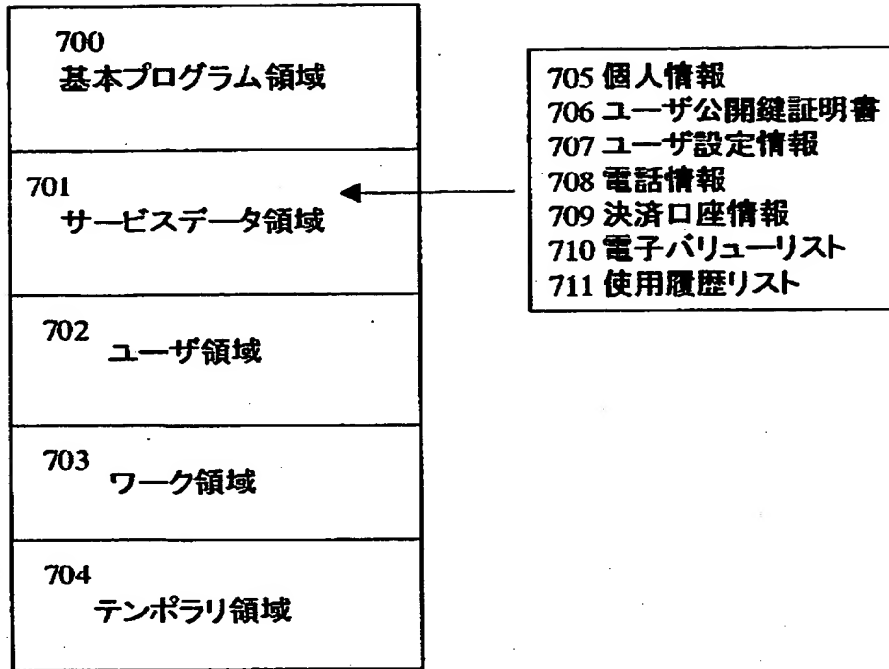
【図 5】

500 サービスデータ
502 マーチャント情報 503 マーチャント公開鍵証明書 504 マーチャント設定情報 505 電話情報 506 決済口座情報 507 対象電子バリューリスト 508 コンテンツリスト 509 トランザクション履歴リスト
501 コンテンツデータ

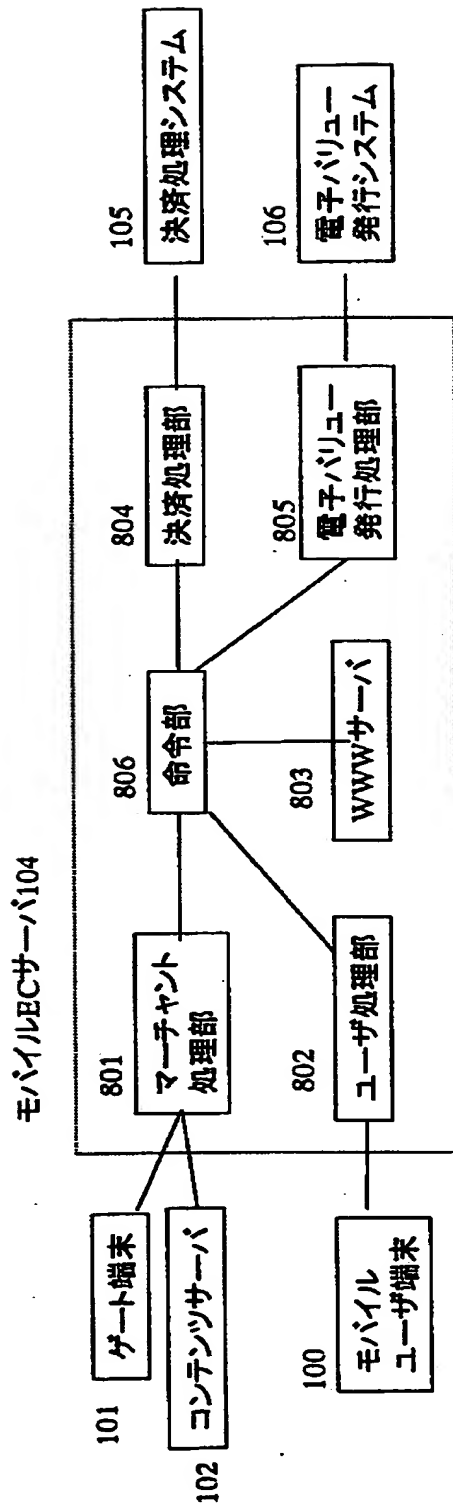
【図 6】



【図 7】



【図 8】



【図 9】

900 ユーザ名
901 ユーザID
902 個人情報
903 ユーザ公開鍵証明書
904 端末情報
905 ユーザ設定情報
906 電話情報
907 決済口座情報
908 電子バリューリスト
909 使用履歴リスト

【図 1 0】

1000 マーチャント名
1001 マーチャントID
1002 ゲート端末ID/コンテンツサーバID
1003 マーチャント情報
1004 マーチャント公開鍵証明書
1005 端末情報
1006 マーチャント設定情報
1007 電話情報
1008 決済口座情報
1009 対象電子バリューリスト
1010 トランザクション履歴リスト

【図 1 1】

1100 決済処理機関名
1101 決済処理機関ID
1102 決済処理機関情報
1103 決済処理機関公開鍵証明書
1104 決済履歴リスト

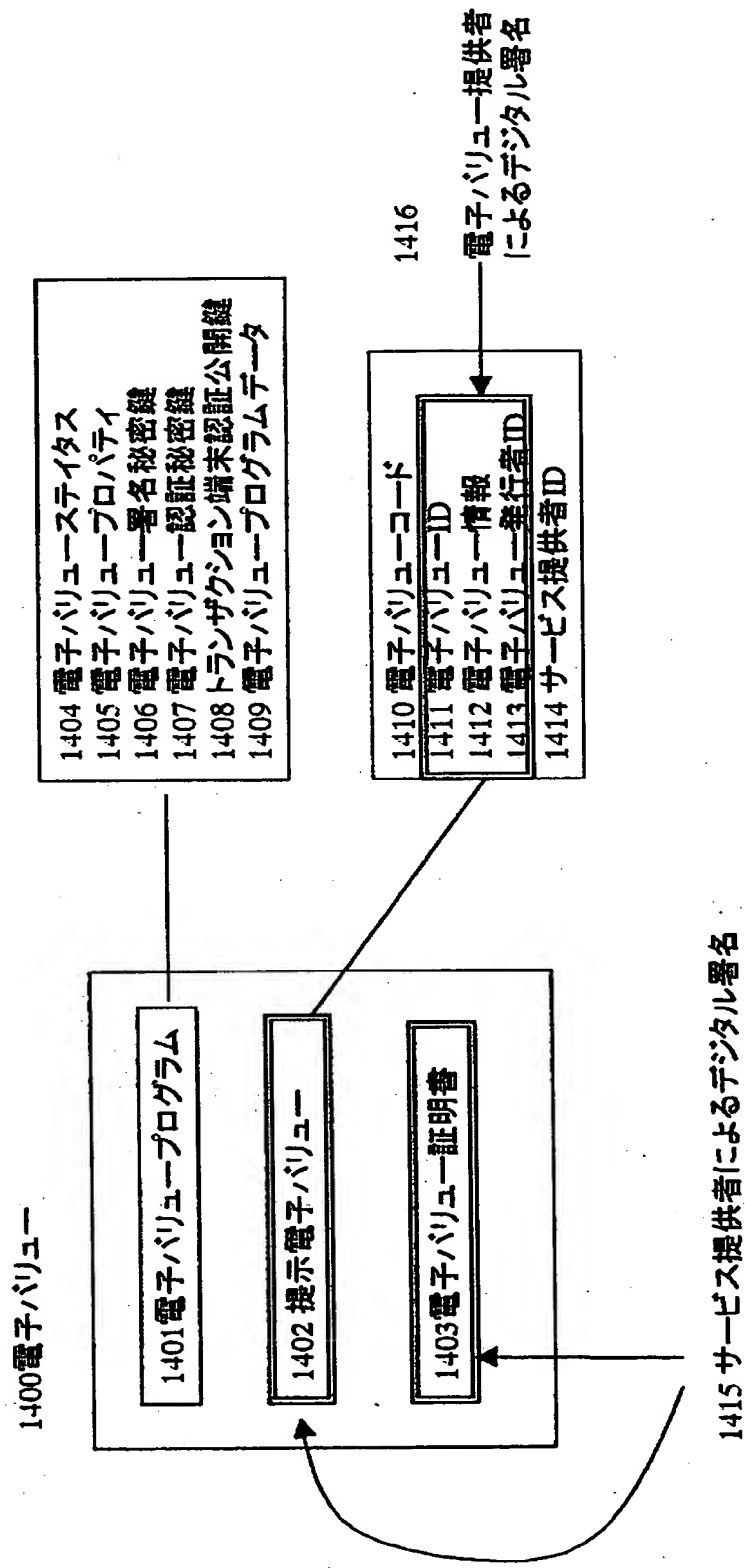
【図 12】

1200	電子バリュー発行者名
1201	電子バリュー発行者ID
1202	電子バリュー発行者情報
1203	電子バリュー発行者公開鍵証明書
1204	サービスコードリスト
1205	トランザクション履歴リスト

【図 13】

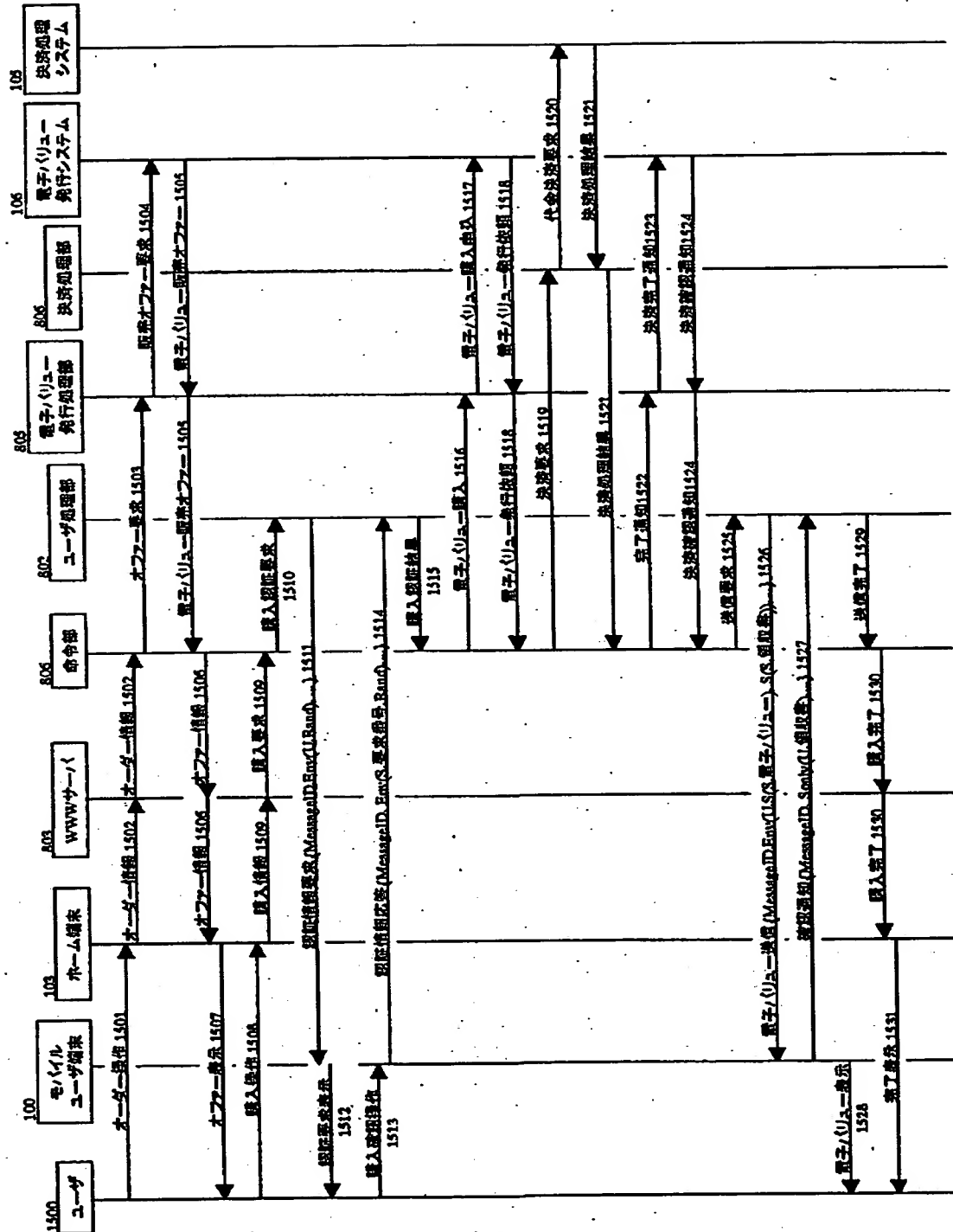
1300	ユーザリスト
1301	マーチャントリスト
1302	決済処理機関リスト
1303	電子バリュー発行者リスト
1304	WWWサーバ情報
1305	サービス提供履歴リスト
1306	電子バリュー管理情報

【図 1 4】

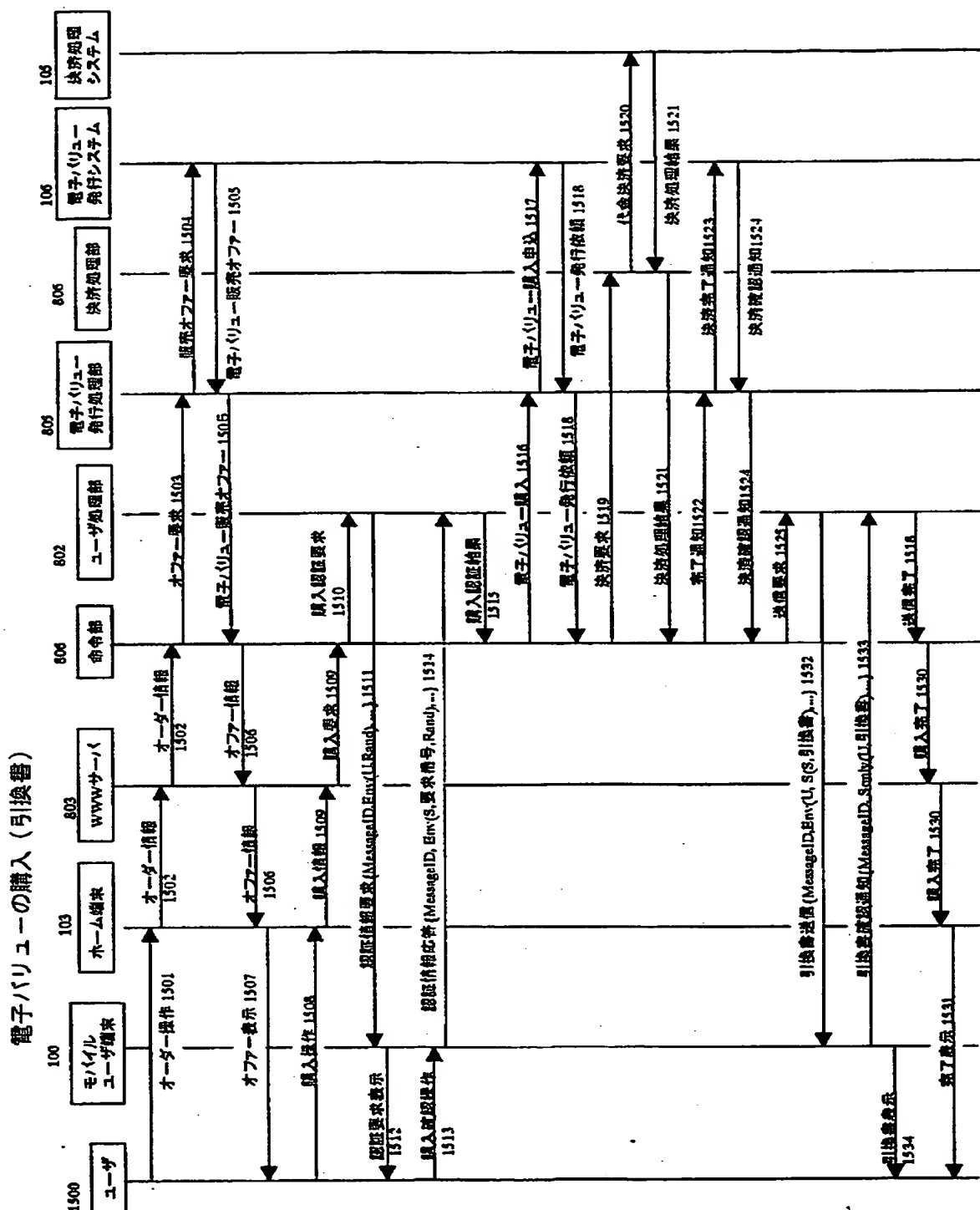


【図15】

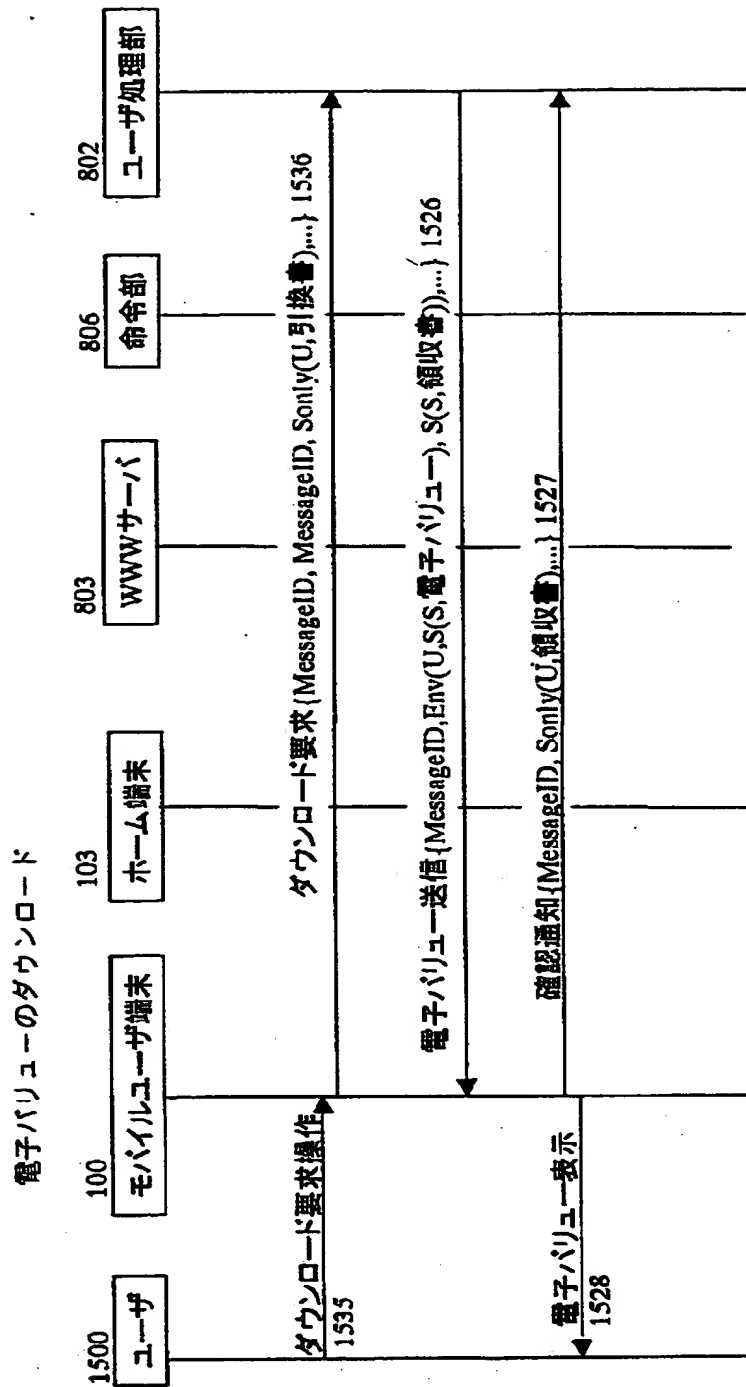
電子バリュウの購入



【图 16】



【図 1 7】



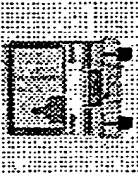
【図 1 8】

(d)電子バリュー表示 1528

603

電子バリュー

バス乗車回数券



残量:10枚

(c)認証要求表示 1510

603

電子バリュー

購入実行

バス乗車回数券(10枚)
金額:1500円

購入を実行する場合、
実行キーを押してください。

(a)オーダー画面

ホーム端末テレビモニタ202

オーダー

☐バス乗車回数券(5枚)

☒バス乗車回数券(10枚)

☐バス乗車回数券(20枚)

注文 キャンセル

(b)オフアー表示 1504

ホーム端末テレビモニタ202

販売オフアー

バス乗車回数券(10枚)
金額:1500円

ユーザID

購入 キャンセル

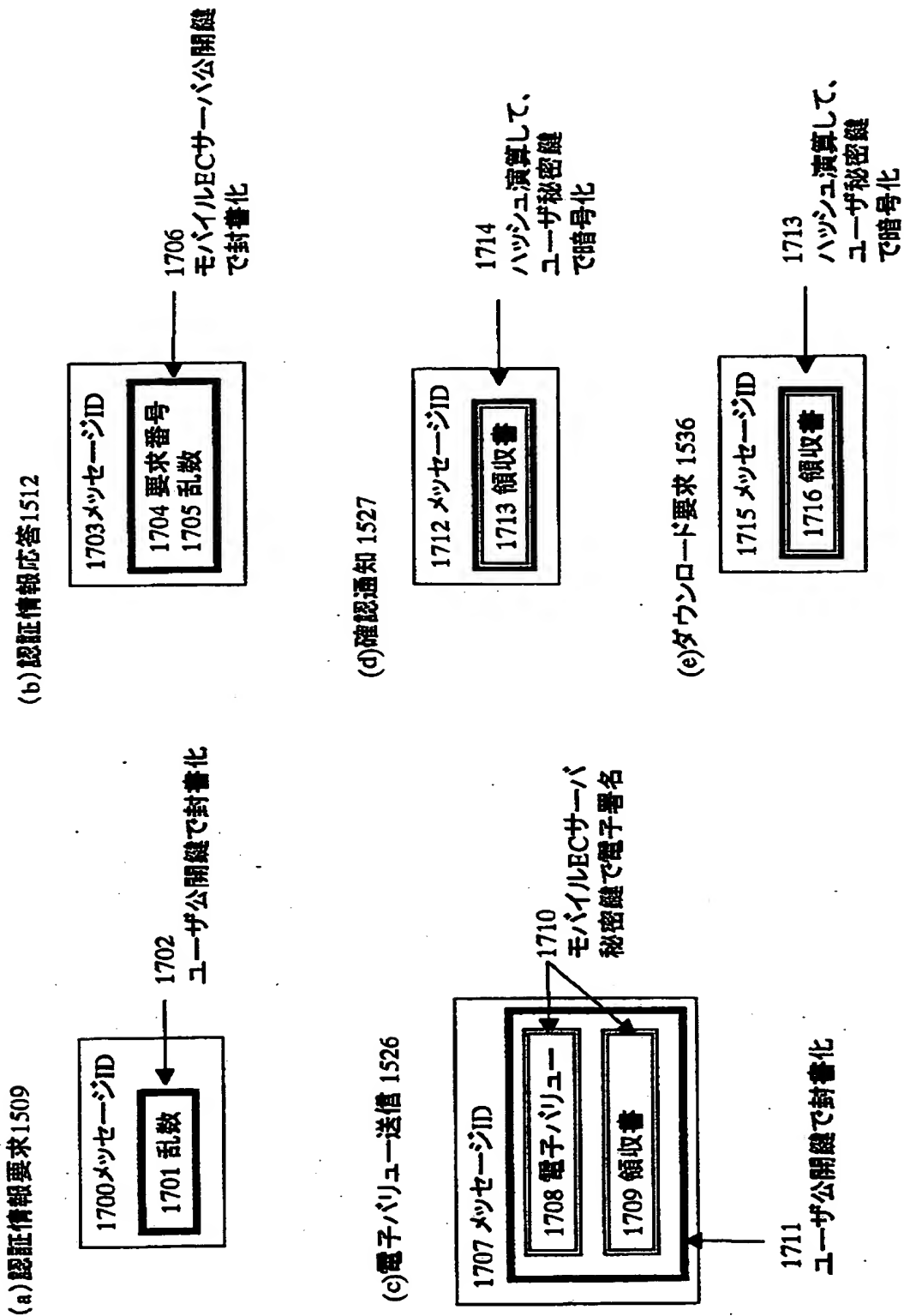
(e)完了表示 1531

ホーム端末テレビモニタ202

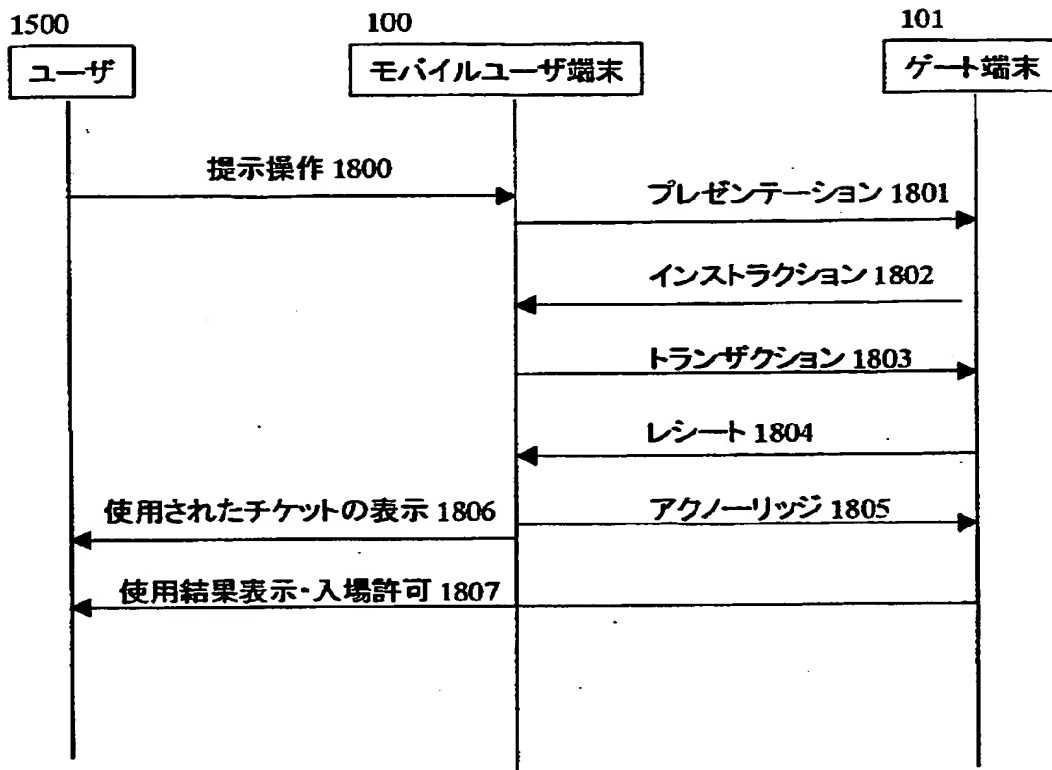
購入処理は完了しました。
ご利用ありがとうございました。

バス乗車回数券(10枚)
金額:1500円

【図 1 9】

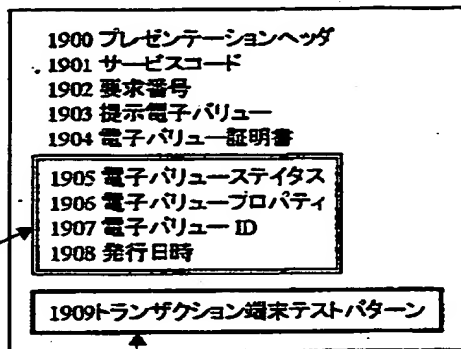


【図 2 0】



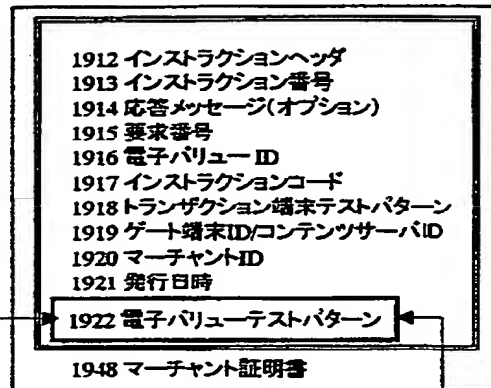
【図 21】

(a) プレゼンテーションのデータ構造



1910 トランザクション端末認証公開鍵で暗号化
1911 電子バリュー署名秘密鍵で署名

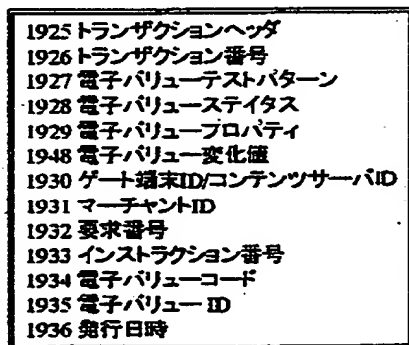
(b) インストラクションのデータ構造



1924 マーチャント秘密鍵で署名

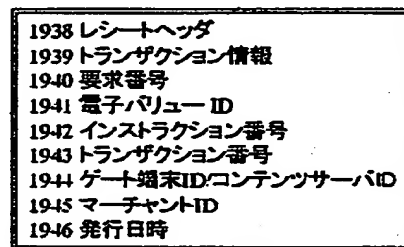
1923 電子バリュー認証公開鍵で暗号化

(c) トランザクションのデータ構造



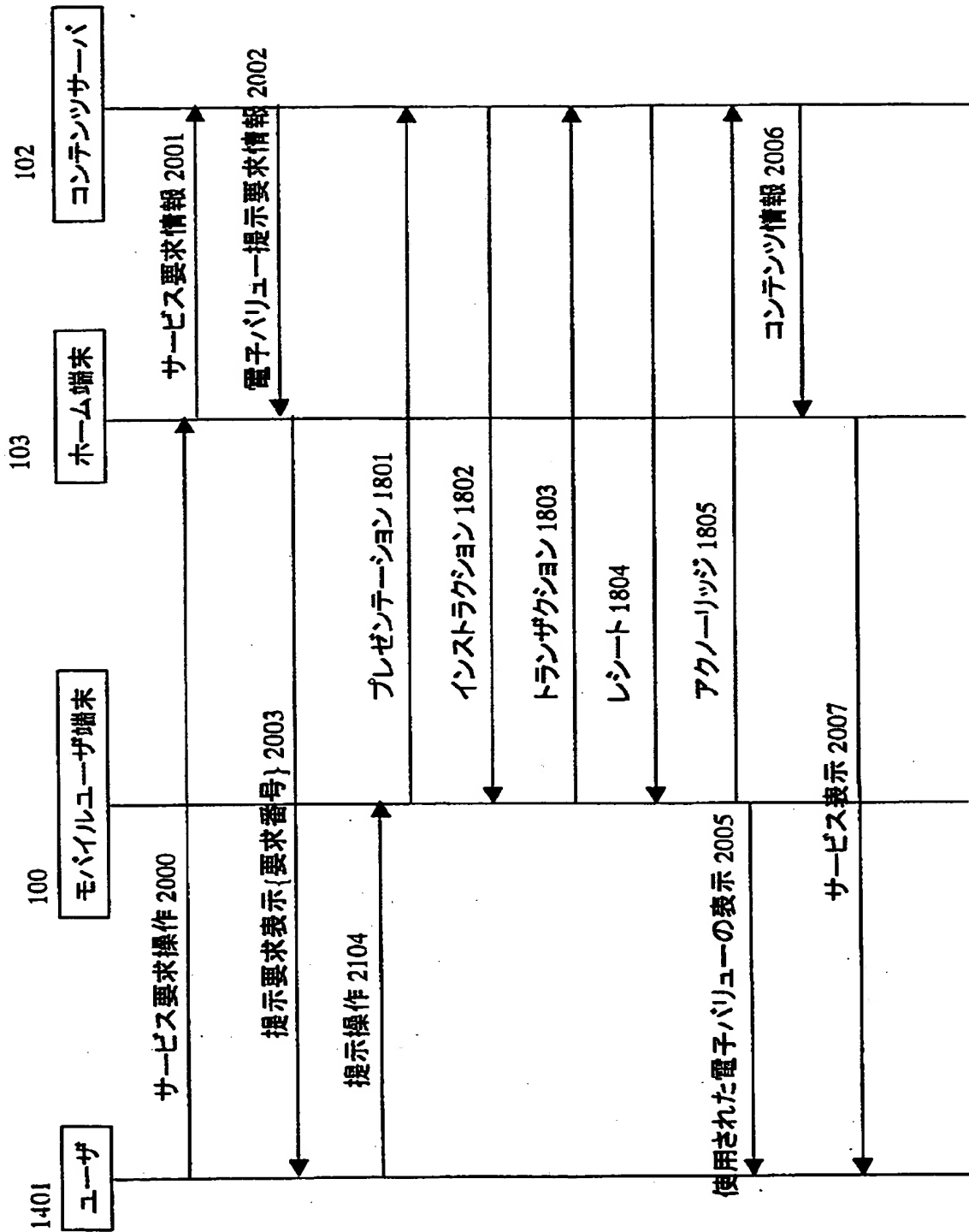
1937 電子バリュー署名秘密鍵で署名・ユーザ秘密鍵で署名

(d) レシートのデータ構造

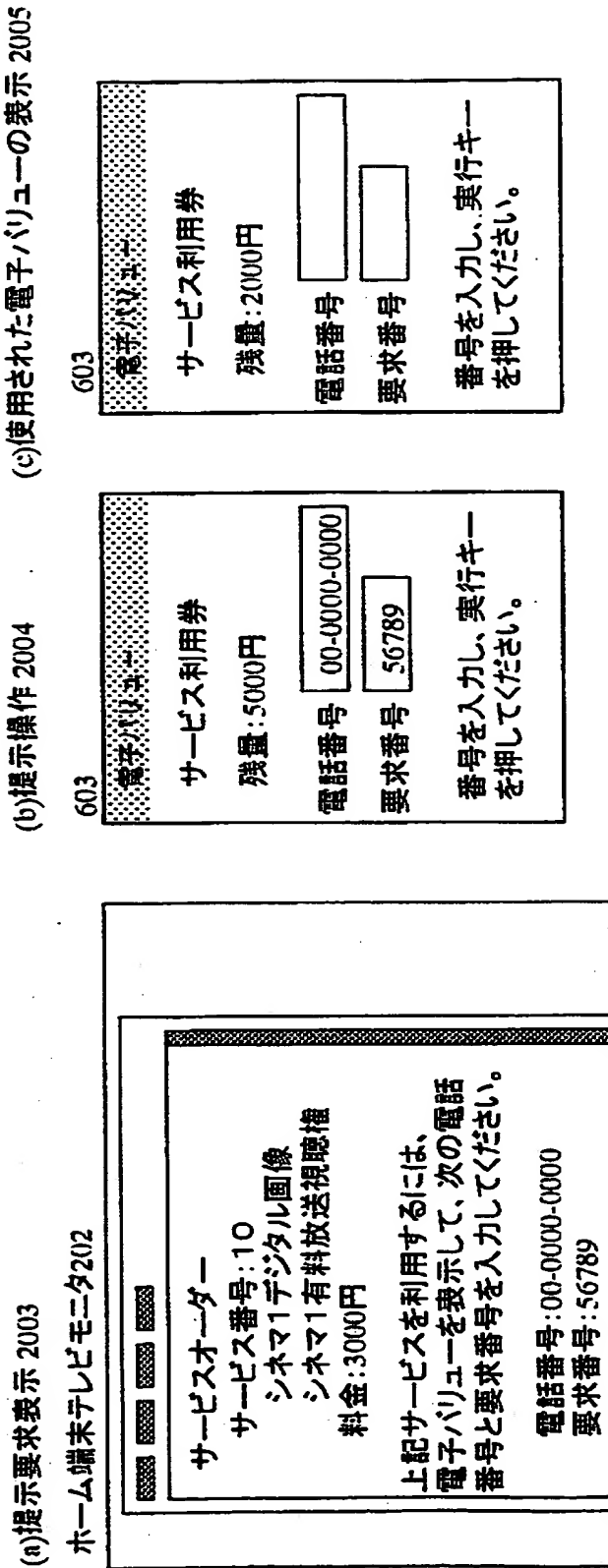


1947 マーチャント秘密鍵で署名

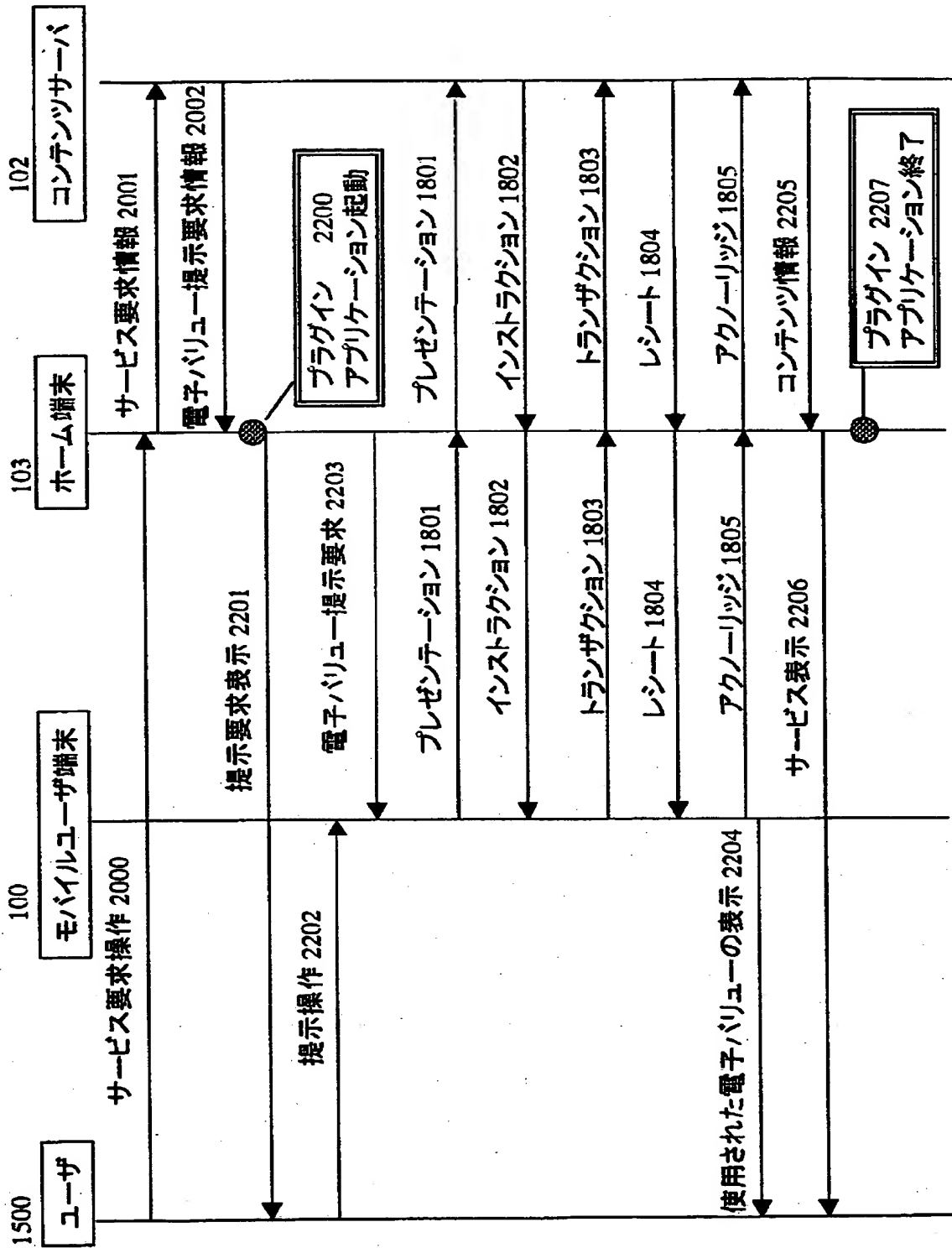
【図 2 2】



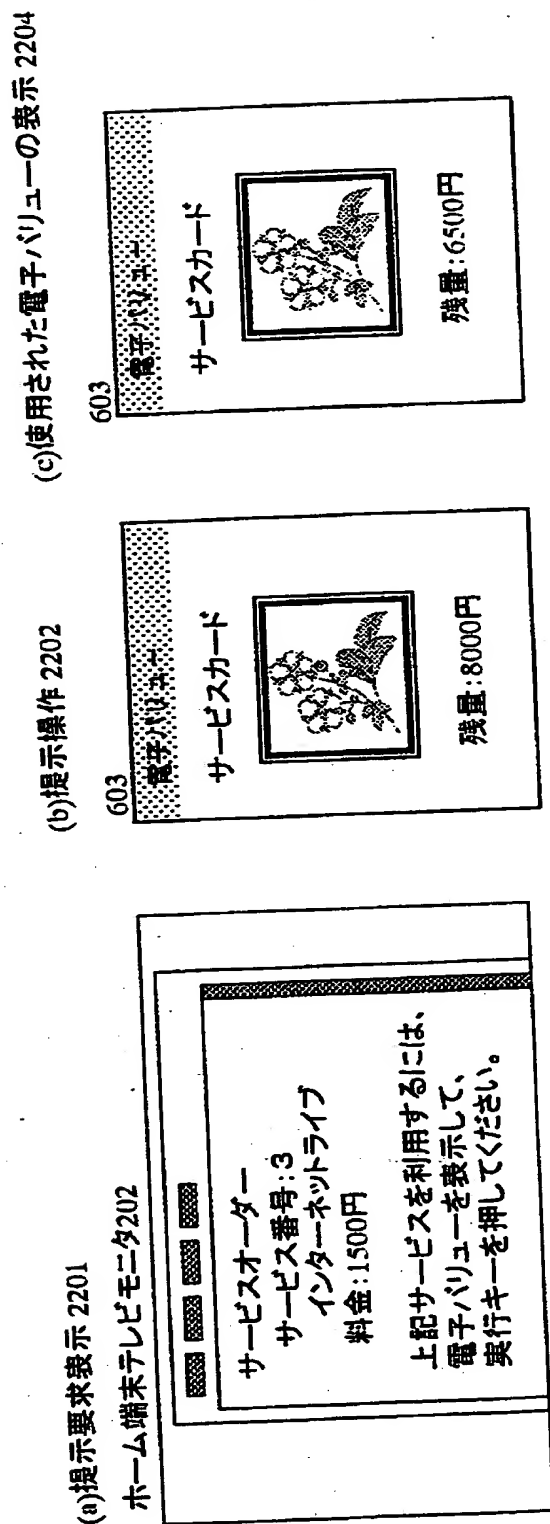
【図 2 3】



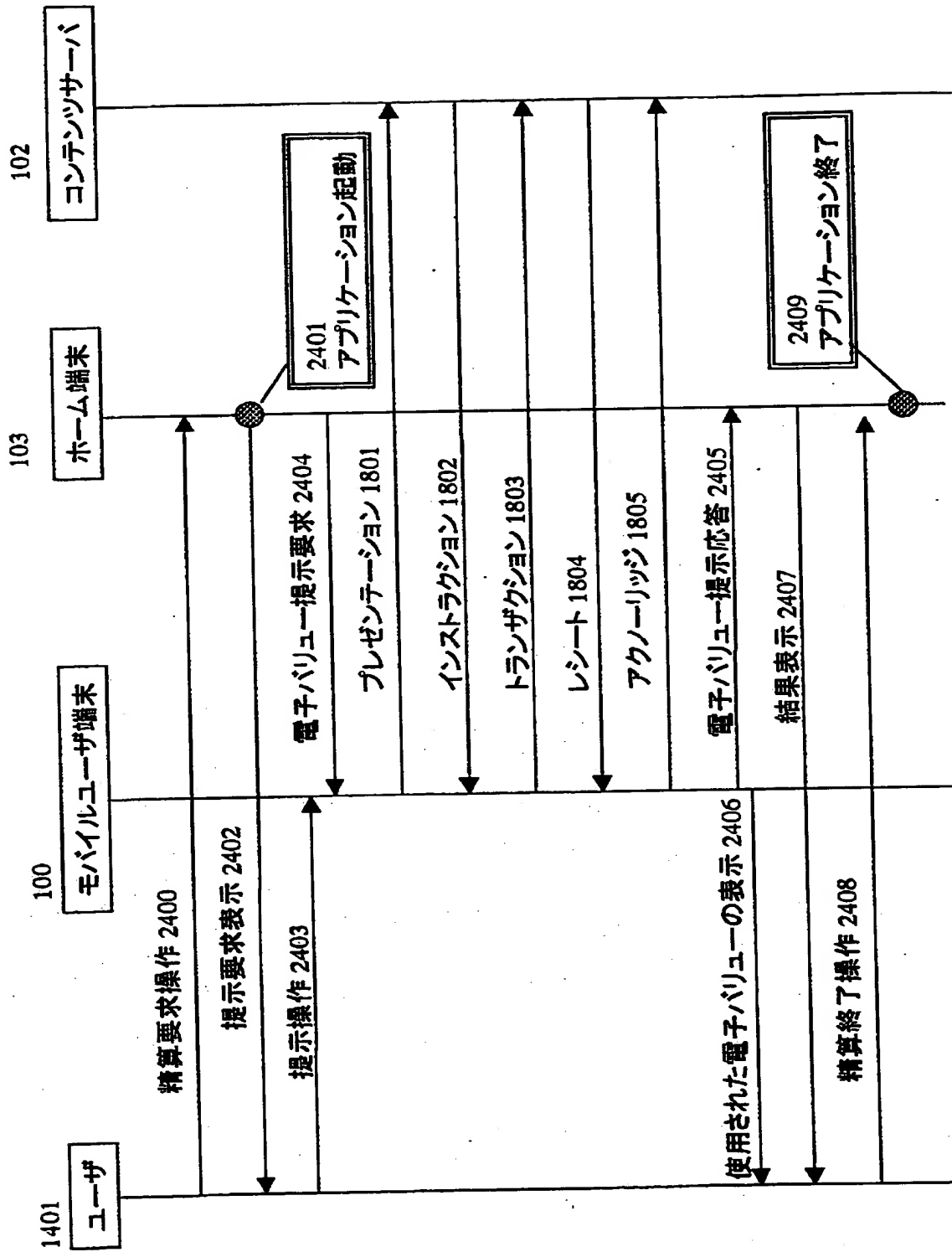
【図 2 4】



【図 2 5】



【図 26】



【図27】

(a)提示要求表示 2403

ホーム端末テレビモニタ202

現在の課金情報
合計:6500円(8番組視聴)
前回支払い日:○年○月○日

支払を実行するには、
電子バリューを表示して、
実行キーを押してください。

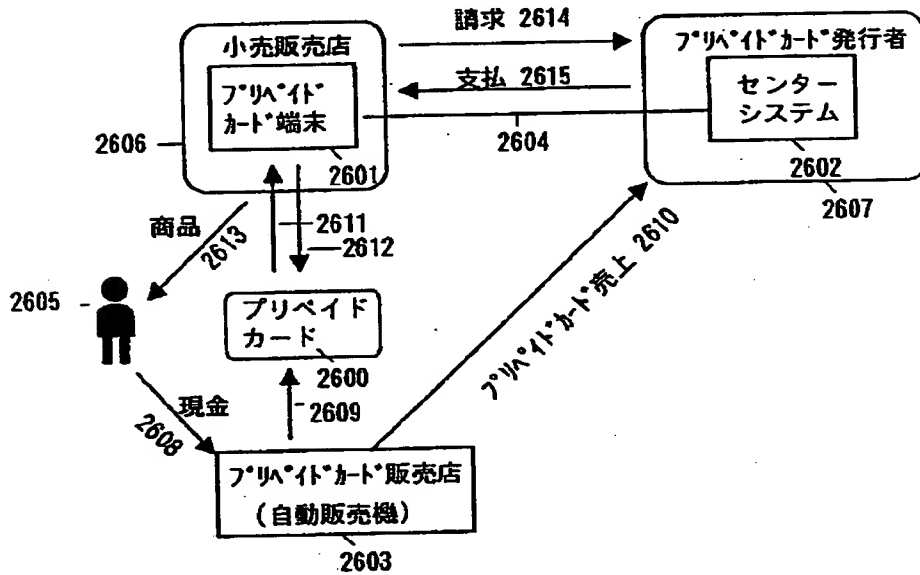
(a)結果表示 2409

ホーム端末テレビモニタ202

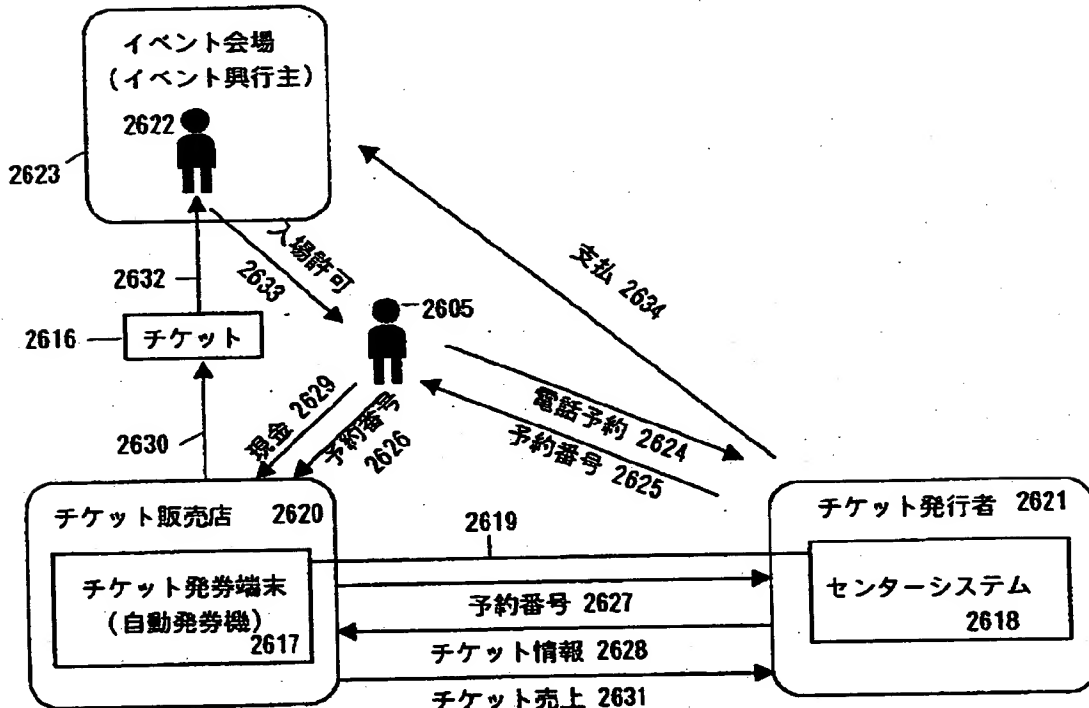
現在の課金情報
合計:0円(0番組視聴)
前回支払い日:△年△月△日

【図 28】

(a) 従来のプリペイドカードを用いた前払い方式による決済システム



(b) 従来の電子バリュー販売システム



【書類名】 要約書

【要約】

【課題】 安全性と利便性とに優れたモバイル・エレクトロニックコマース・システムを提供することを目的とする。

【解決手段】 ホーム端末103からのオーダーに対し、モバイルECサーバ104は、ユーザ認証を行ない、あらかじめ登録されたユーザのモバイルユーザ端末100に、オーダーされた電子バリューをデジタル無線電話通信で送信する。モバイルユーザ端末100は、電子バリューを内部に格納し、デジタル無線電話通信で、コンテンツサーバ102と決済情報を交換し、ホーム端末103に提供される有料情報サービスや有料放送の代金を支払う。

【選択図】 図 1